54Mbps Wireless-G Router

CWR-854

User's Guide

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

FCC CAUTION 3
SAFE SEATING GESTURES 3
CE STATEMENT OF CONFORMITY 3
CHAPTER-1 INTRODUCTION 4
1.1 PACKAGE CONTENT 4
1.2 SPECIFICATION 5
1.3 FEATURES 6
1.4 LED INDICATOR 7
1.5 REAL PANEL DESCRIPTION 8
CHAPTER-2 INSTALLATION 9
2.1 HARDWARE INSTALLATION 9
2.2 PREPARING THE NETWORKING 10
2.3 COLLECTING ISP INFORMATION 10
2.4 CONFIGURING WINDOWS FOR IP NETWORKING 10
CHAPTER-3 WEB CONFIGURATION 16
3.1 SETUP WIZARD 16
3.1.1.Operation Mode *17*
3.1.2 Time Zone Settings *18*
3.1.3 LAN Interface Setup *19*
3.1.4 WAN Interface Setup *20*
3.1.5 Wireless Basic Settings *21*
3.1.6 Wireless Security Setup *22*
3.2 OPERATION MODE 23
3.3 WIRELESS 24
3.3.1 Basic Settings *24*
3.3.2 Wireless Advanced Settings *26*
3.3.3 Security *28*
3.3.4 Access Control *33*
3.3.5 WDS Settings *34*
3.3.6 Site Survey *35*
3.3.7 WPS *36*
3.4 TCP / IP SETTINGS 37
3.4.1 LAN Interface *37*
3.4.2 WAN Interface *39*
3.5 FIREWALL 47
3.5.1 Port Filtering *47*
3.5.2 IP Filtering *48*
3.5.3 MAC Filtering *49*
3.5.4 Port Forwarding *50*
3.5.5 URL Filtering *51*
3.5.6 DMZ *52*
3.6 MANAGEMENT 53
3.6.1 Status *53*
3.6.2 Statistics *54*
3.6.3 DDNS *55*
3.6.4 Time Zone Settings *56*
3.6.5 Denial of Service (DoS Prevention) *57*
3.6.6 Event Log *58*
3.6.7 Upgrade Firmware *59*
3.6.8 Save / Reload Settings *60*
3.6.9 Password *61*
APPENDIX A: TROUBLESHOOTING 62
APPENDIX B: FREQUENTLY ASKED QUESTIONS 65

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

FCC Caution

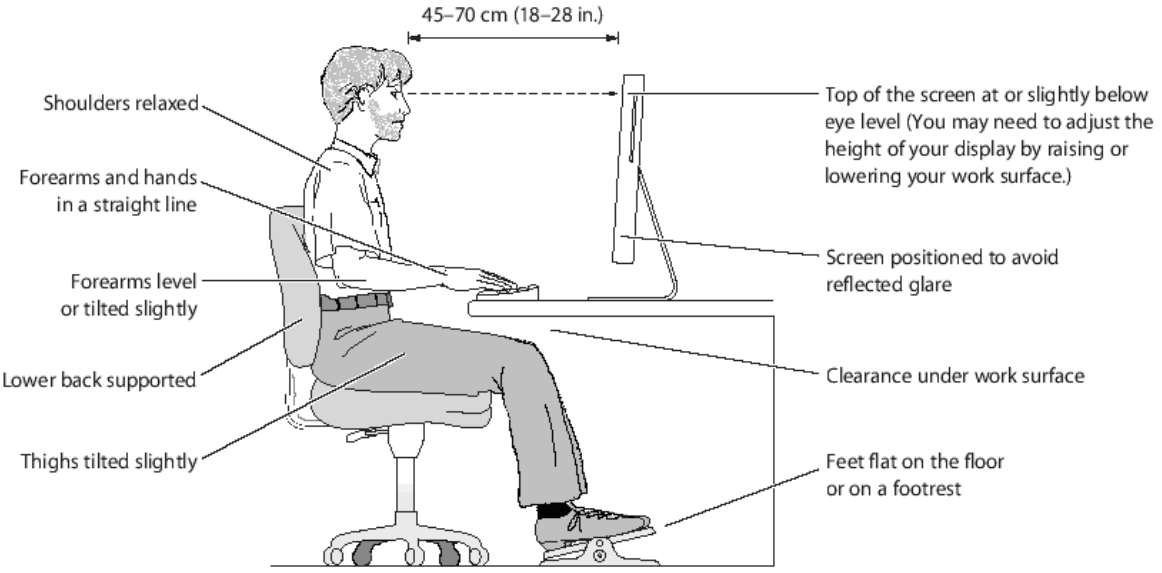
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

Safe Seating Gestures

The user have to choose an adjustable chair, comfortable is the key. You should follow the manufacturer's instructions for adjusting the backrest to fit your body properly. Following is the explanation of the picture.

- λ Shoulders relaxed, and forearms and hands in a straight line.
- λ Lower back support and thighs tilted slightly.
- λ Top of the screen at or slightly below eye level.
- λ Screen positioned to avoid reflected glare.
- λ Clearance under work surface.
- λ Feel flat on the floor.
- λ The distance between you and the monitor should be 45~70 cm（18~28 inch）


45–70 cm (18–28 in.)
Shoulders relaxed
Forearms and hands in a straight line
Forearms level or tilted slightly
Lower back supported
Thighs tilted slightly
Top of the screen at or slightly below eye level (You may need to adjust the height of your display by raising or lowering your work surface.)
Screen positioned to avoid reflected glare
Clearance under work surface
Feet flat on the floor or on a footrest

CE Statement of Conformity

Our product has been tested in typical configuration by Ecam Sertech Corp and was found to comply with the essential requirement of "Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility" (89/336/EEC; 92/31/EEC; 93/68/EEC)

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

Chapter-1 Introduction

Thank you for choosing the CNet Wireless series product. CWR-854 is an ideal Wireless-G Router for the small office or home networking environments. Setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN. CWR-854 is not only a Wireless Router but also supports AP Client / Bridge and WDS (Wireless Distributed System) mode to satisfy all kinds of the application from different networking environment. The WPS (Wi-Fi Protected Setup) function could help you establish a wireless home network easily and securely.

CWR-854 also provides step-by-step installation for both Internet setting as well as LAN and Wireless connection. For Wireless security that the router supports WEP, WPA and WPA2 (TKIP/AES), and CWR-854 also equipped with advanced MAC address, IP/Port Filtering and URL Filtering to safe and secure home or office network.

This router can be easily configured without other utility install. You could just follow this user manual to setup your Wireless Network with the embedded GUI browser.

1.1 Package Content

The package of CWR-854 includes the following items,

- **1 x CWR-854**
- **1 x Power Adapter**
- **1 x Documentation CD**
- **1 x RJ-45 Cable Line**
- **1 x Detachable Antenna**
- **1 x Cradle**
- **1 x QIG**

Notes: If any of above items are missing, please contact with your supplier as soon as possible.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

1.2 Specification

Standard	IEEE 802.11G/B
Frequency Band	2.400GHz ~ 2.484GHz
Radio Type	IEEE 802.11g: OFDM (64-QAM, 16-QAM, QPSK, BPSK) IEEE 802.11b: DSSS (CCK/DQPSK/DBPSK)
Data Rate (Wireless)	802.11g: 54 / 48 / 36 / 24 / 18 / 12 / 9 & 6Mbps 802.11b: 11 / 5.5 / 2 & 1 Mbps with auto-rate fall back
Access Protocol	CSMA/CA
Number of Operation Channel	2.412~2.462GHz (Canada, FCC) / 11 Channels 2.412~2.484GHz (Japan, TELEC) / 14 Channels 2.412~2.472GHz (Euro, ETSI) / 13 Channels
Operation Mode	AP AP Client (ad-hoc and infrastructure) Client Bridge (point-to-pint and point-to-multipoint) WDS (Wireless Description System)
Security	64/128bit WEP WPA (TKIP with IEEE 802.1x) WPA2 (AES with IEEE 802.1x)
RF Output Power (Typical)	802.11g: up to 14 ± 1 dBm 802.11b: up to 17 ± 1 dBm
Sensitivity	-68dBm @ 802.11g -80dBm @ 802.11b
Antenna	One detachable 5dbi antenna
Dimension (L x W x H)	165 x 118 x 27mm (6.49 x 4.65 x 1.06inch)
Weight	245g
Operation Temperature	0°C ~ 40°C (32° ~ 104°F)
Storage Temperature	-20°C ~ 60 °C (-4° ~ 140°F)
Humidity	10% ~ 90% (Non-condensing)
Connector	One antenna connector One RJ-45 port for WAN Four RJ-45 LAN ports Reset to default button WPS button Power jack
Power requirement	12V DC, 1A

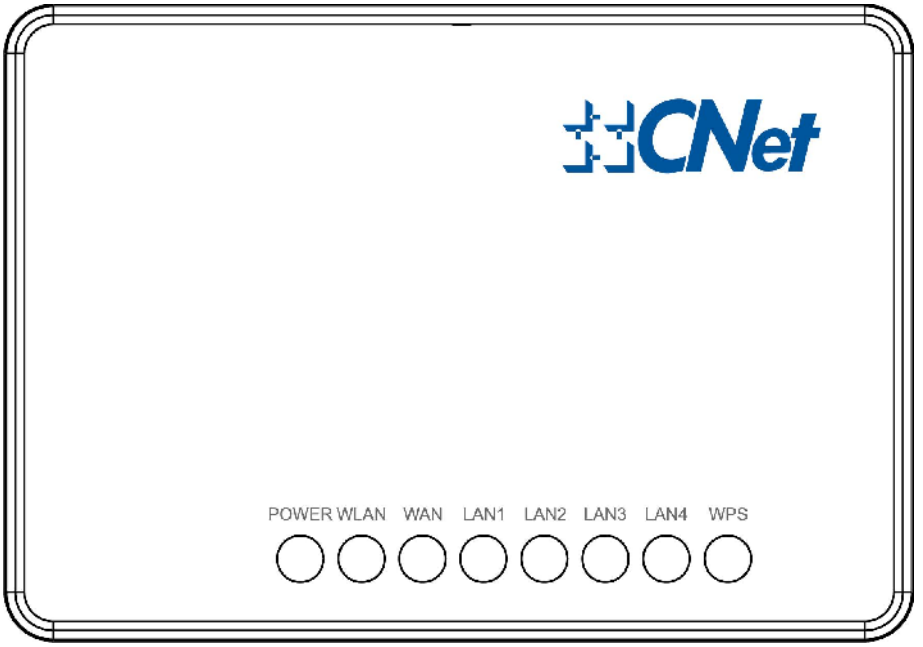
Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

1.3 Features

- 802.11b/g compliant with 54Mbps high-speed data rate
- Operation modes: AP, AP client, Client, Bridge, WDS
- DHCP Server/Client
- Four Ethernet ports for broadband sharing
- Virtual DMZ, Port Forwarding
- Dynamic DNS
- TCP/UDP/ICMP/ARP protocol stack
- Firewall, URL/IP/Port/MAC filtering
- Wireless users access control
- Wireless security – 64/128bit WEP, WPA/WPA2, 802.1x and 802.11i
- Support PPPoE, VPN pass-through with multiple sessions, PPTP and L2TP
- Universal Plug and Play, no complicated installation necessary
- Quick and easy setup with Web-based management utility
- Detachable antenna allows user to replace higher gain antenna
- Supports WPS, 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

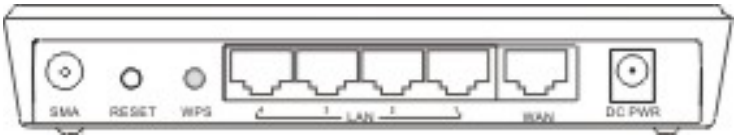
1.4 LED Indicator



LED Indicator	State	Description
POWER	ON	The WLAN Broadband Router is powered on
	OFF	The WLAN Broadband Router is powered off
WLAN	Flashing	Data is transmitting or receiving on the antenna
	OFF	No data is transmitting or receiving on the antenna
WAN	Flashing	Data is transmitting or receiving on the LAN interface
	ON	Port linked
	OFF	No link
LAN 1~4	Flashing	Data is transmitting or receiving on the WAN interface
	ON	Port linked
	OFF	No link
WPS	ON	WPS function is waiting for the registration from client side
	OFF	WPS function is off

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

1.5 Real Panel Description



Interfaces	Description
Antenna (Fixed / SMA)	The Wireless LAN Antenna.
Reset	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.
WPS	Push continually the WPS button 5 ~ 10 seconds to enable the WPS feature.
LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Supports auto-sensing on 10/100M speed and half / full duplex, and comply with IEEE 802.3 / 802.3u respectively.
WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Supports auto-sensing on 10/100M speed and half / full duplex, and comply with IEEE 802.3/ 802.3u respectively.
Power	The power jack allows an external power supply connection.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

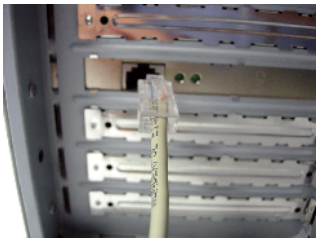
Chapter-2 Installation

2.1 Hardware Installation

1. Place the Wireless LAN Broadband Router to the best optimum transmission location. The best transmission location for your WLAN Broadband Router is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.

2. Connect the **WAN port** on the router to a **Cable/DSL** modem, Ethernet Server, or hub.

3. Connect one or more client PCs to the **LAN port(s)**.



4. Connect the power adapter to the wall outlet and the **power jack** on the router.

5. Turn your PCs on.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

2.2 Preparing the Networking

This chapter covers the things that need to be done before configuring the router. The first thing is to set all computers on the network for TCP/IP networking and also gather necessary information from the Internet Service Provider (ISP).

2.3 Collecting ISP Information

The following information needs to be gathered from the ISP before configuring the router:

- IP Assignment from ISP: Are IPs assigned dynamically or you have a fixed IP address? If fixed, what are the IP address, Subnet Mask, Default Gateway as well as the DNS addresses for this account?
- Connection Type: Is this a PPPoE or PPTP connection? If PPPoE, what are the username and password associated with this account? If PPTP, the server IP address as well as user authentication information is required.

  Please contact your ISP if you're not sure of the answers to these questions.

2.4 Configuring Windows for IP Networking

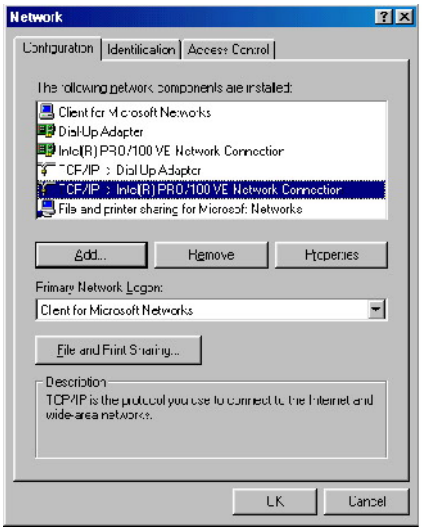
Each computer on the network and connecting to the router should be configured for TCP/IP networking. The router is by default a DHCP server and if you plan to use DHCP (recommended). Each computer must be configured to receive an IP address automatically. See the procedure below.

If fixed IP addresses are to be used on the network, you'll need to manually assign an IP address to each computer and make sure that they are in the same subnet as the router. Refer to your Windows documentation for instructions on IP assignment.

To configure TCP/IP in Windows:

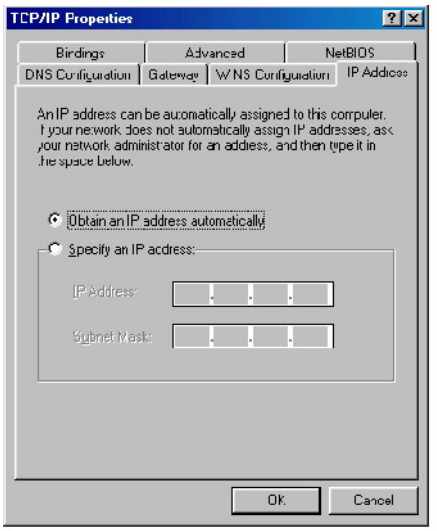
Configuring Windows 98 and millennium PCs

1. Click the **Start** button go to **Settings** and click on **Control Panel.** In Control Panel, double-click the **Network** icon.
2. Under the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. Click the **Properties** button.



Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3. Click the **IP Address** tab. Select **Obtain an IP address automatically.**


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

4. Now click the **Gateway** tab, and verify that the *Installed Gateways* field is Blank. Click the **OK** button.

5. Click the **OK** button again. Windows may ask for original Windows installation CD or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into the CDROM drive and enter the correct file location, e.g., D:\win98, D:\win9x, etc. (“D” is the drive letter of the CD-ROM drive).

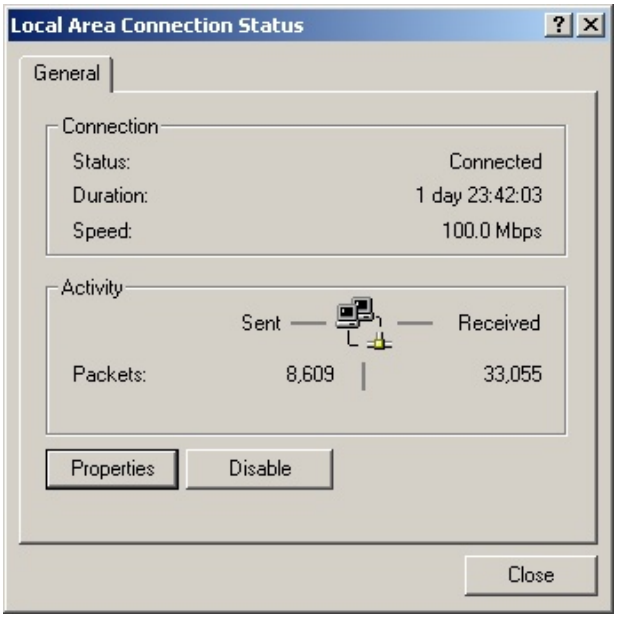
6. Windows may ask to restart the PC. Click the **Yes** button. If Windows does not prompt to restart, restart the computer anyway.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

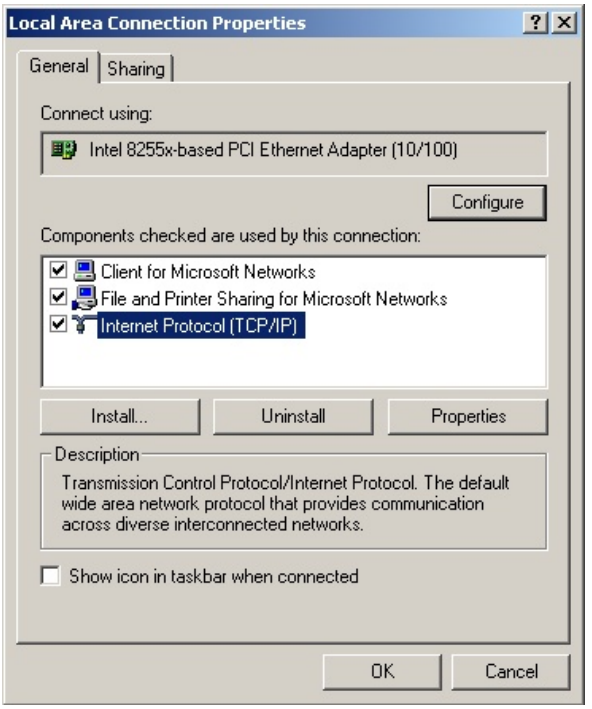
Configuring Windows 2000 PCs

1. Click the **Start** button go to **Settings** and click on **Control Panel**. In Control Panel, double-click the **Network and Dial-up Connections** icon.

2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection and** Click the **Properties** button.

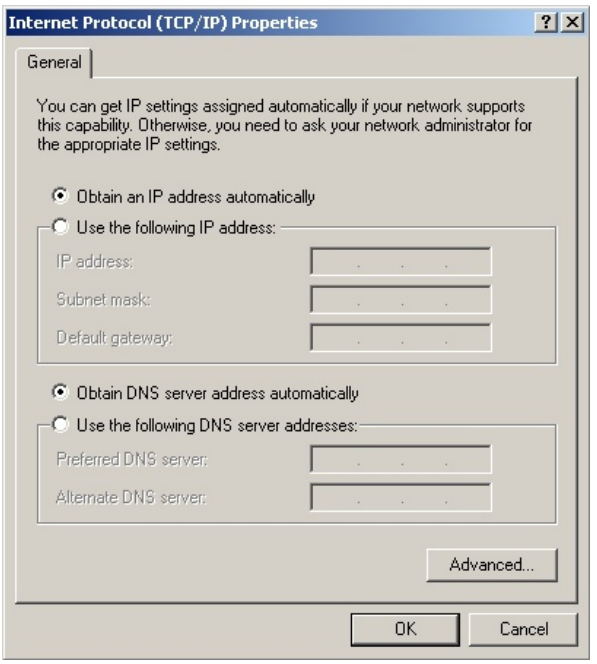


3. Make sure the box next to *Internet Protocol (TCP/IP)* is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

4. Select **Obtain an IP address automatically and** click the **OK** button. Click the **OK** button again to complete the PC configuration.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

5. Restart your computer.

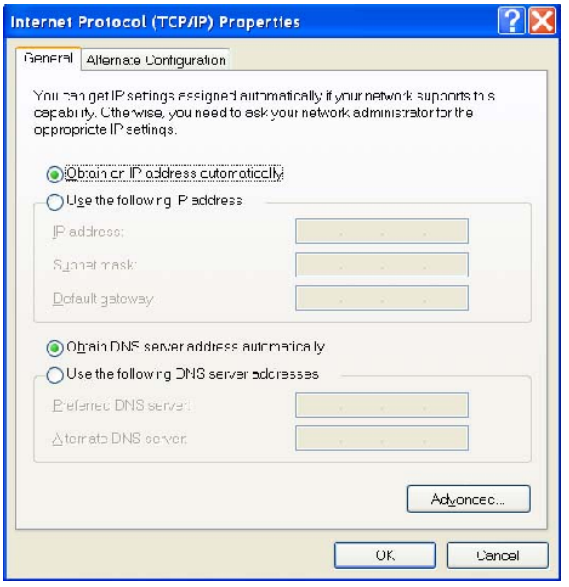
Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

Configuring Windows XP PCs

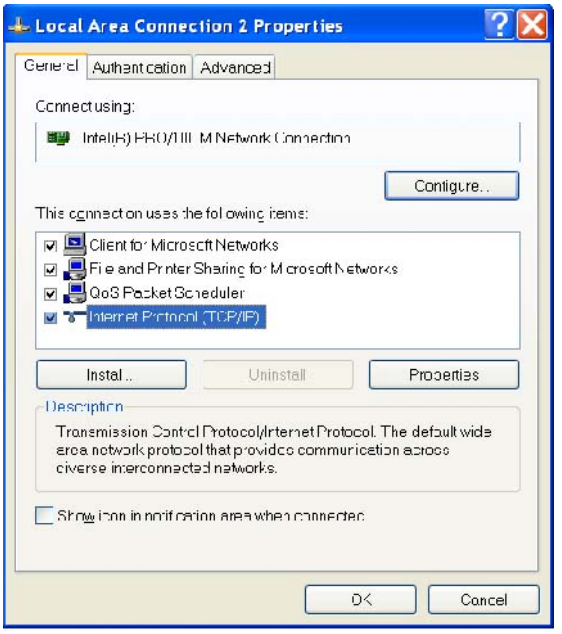
The following instructions assume you are running Windows XP with the default interface (Control Panel looks different then previous versions of Windows). If you are using the Classic View (where icons and menus look similar to previous Windows versions), please follow the instructions for Windows 2000.

1. Click the Start button and then the Control Panel icon. Click the Network and Internet Connections icon. Then click the Network Connections icon.

2. Select the Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the Local Area Connection and click the Properties button.

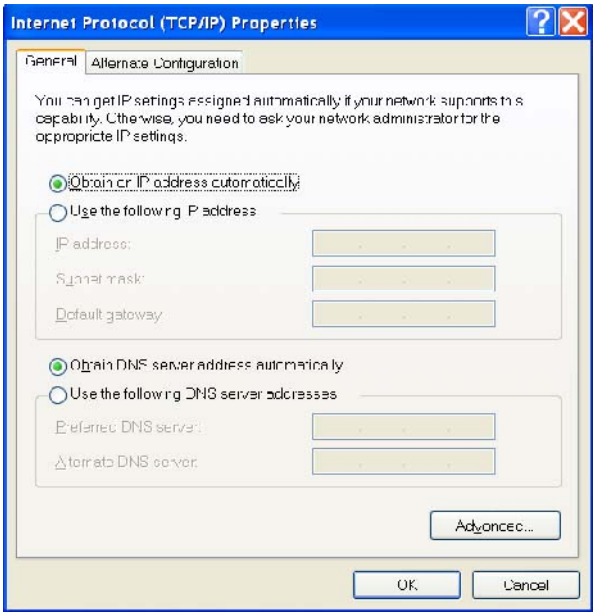


3. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

4. Select **Obtain an IP address automatically** and click OK. Click the **OK** button again to complete the PC configuration.



Configuring Windows XP PCs

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

Chapter-3 Web Configuration

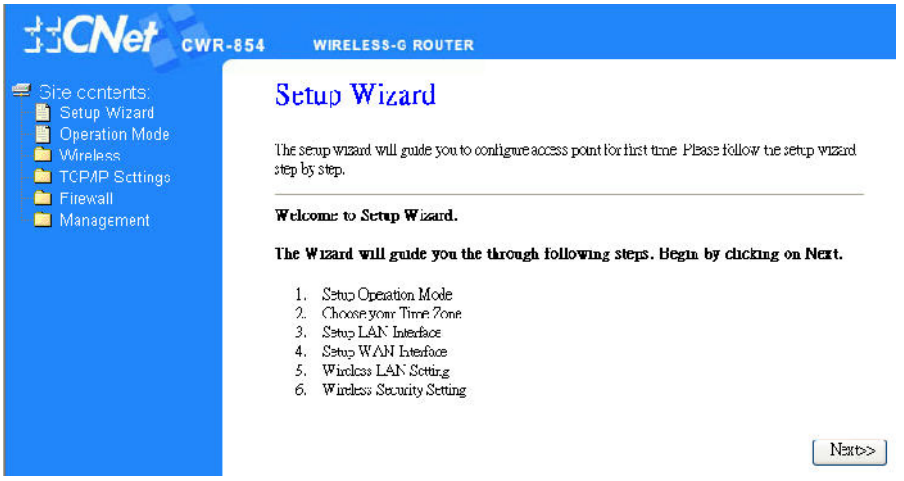
This chapter describes how to access the router through the web browser. Please be noted that in order to access the router's admin page, a computer must be connected to one of the LAN ports on the router.

The WLAN Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: 192.168.1.254
Default IP subnet mask: 255.255.255.0
WEB login User Name: <empty>
WEB login Password: <empty>

3.1 Setup Wizard

After a successful log-in to the router, the setup page will be shown as the below picture.

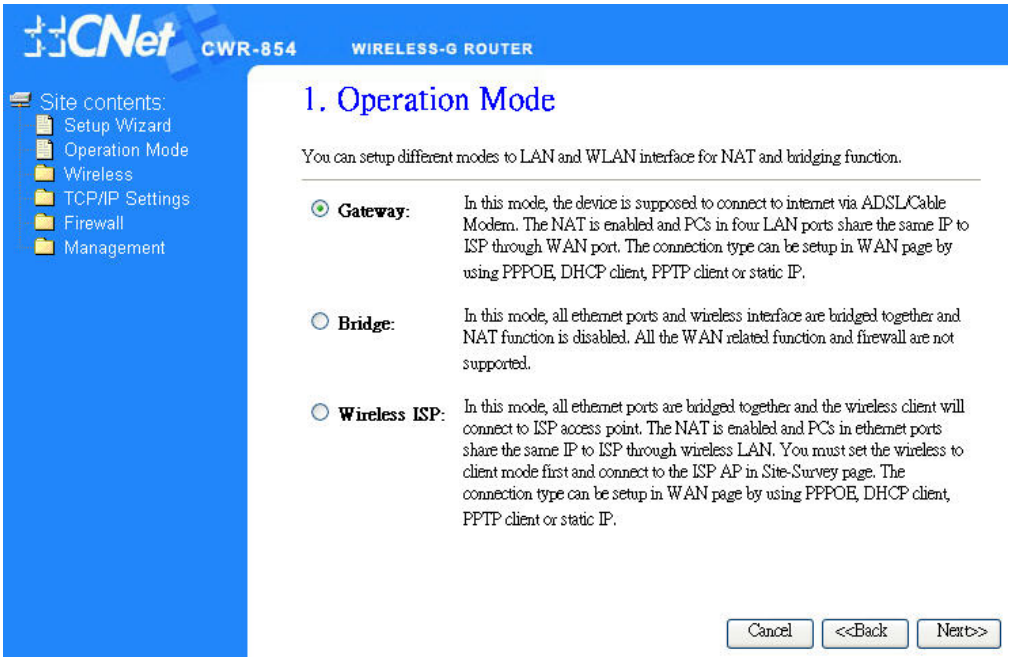


The router's configuration menu provides a Setup Wizard for basic configuration of the router. For more advanced feature settings. Users have to choose different menu items, and then click "**Next"** to proceed with Setup Wizard.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.1.1.Operation Mode

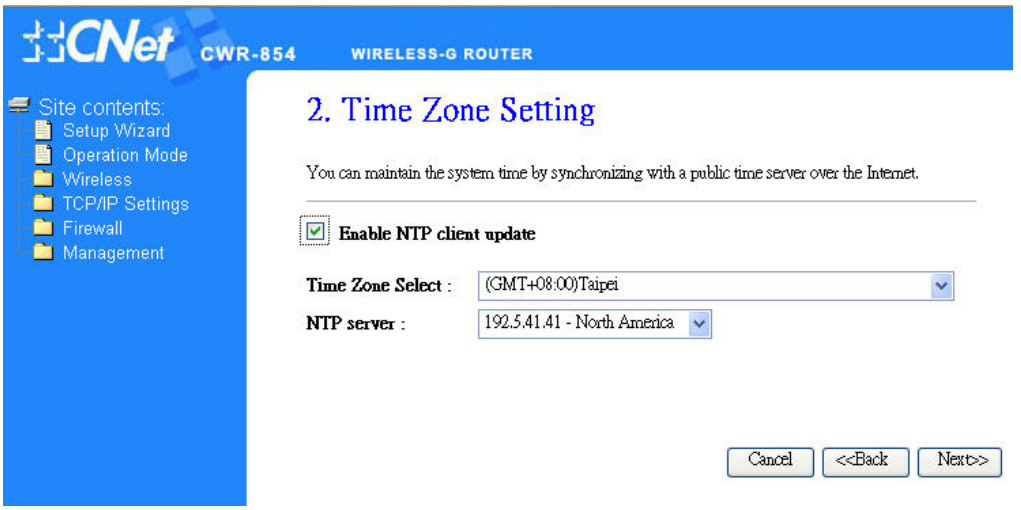
This page followed by Setup Wizard page to define the operation mode. CWR-854 supports three kinds of operation mode for the different application and environment. CWR-854 can be presented a NAT Router, Bridge or Wireless ISP Client.


CNet
CWR-854
WIRELESS-G ROUTER
Site contents:
Setup Wizard
Operation Mode
Wireless
TCP/IP Settings
Firewall
Management
1. Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Bridge:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Cancel
<<Back
Next>>

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.1.2 Time Zone Settings

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.



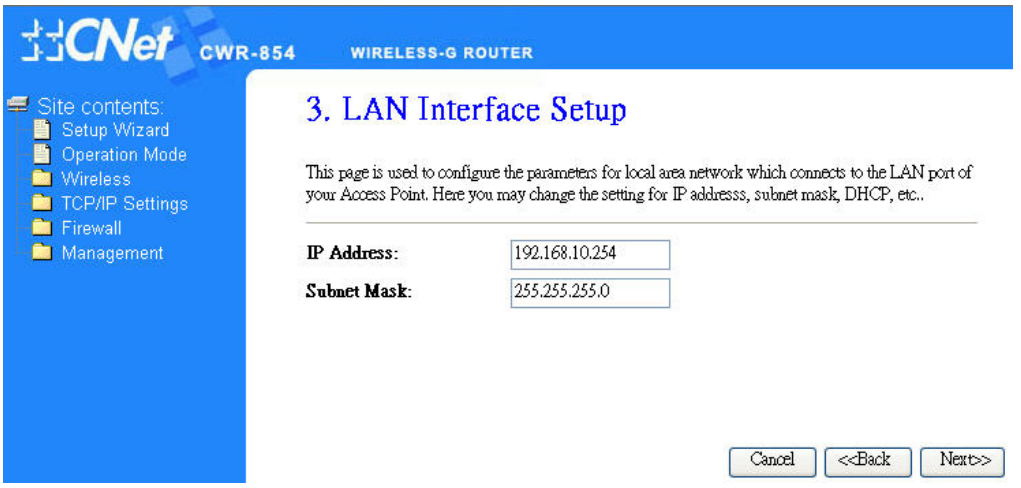
- ✓ **Enable NTP client update**: Enable time zone update function
- ✓ **Time Zone Select**: Select the time zone this router is used in.
- ✓ **NTP serve**r: Select from the list of NTP servers by clicking the down arrow key or manually enter time server IP address.
- ✓ **Cancel**: To skip the current settings and jump to the **Setup Wizard** page.
- ✓ **Back**: To skip the current settings and go back to the last page.
- ✓ **Next:** Go to the next page.

After completing the time zone settings, click "**Next**" to proceed to the LAN Interface Setup page.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.1.3 LAN Interface Setup

In the LAN interface Setup page, users can change the LAN IP address and Subnet Mask of the router. **Most Users will not need to change these values**.



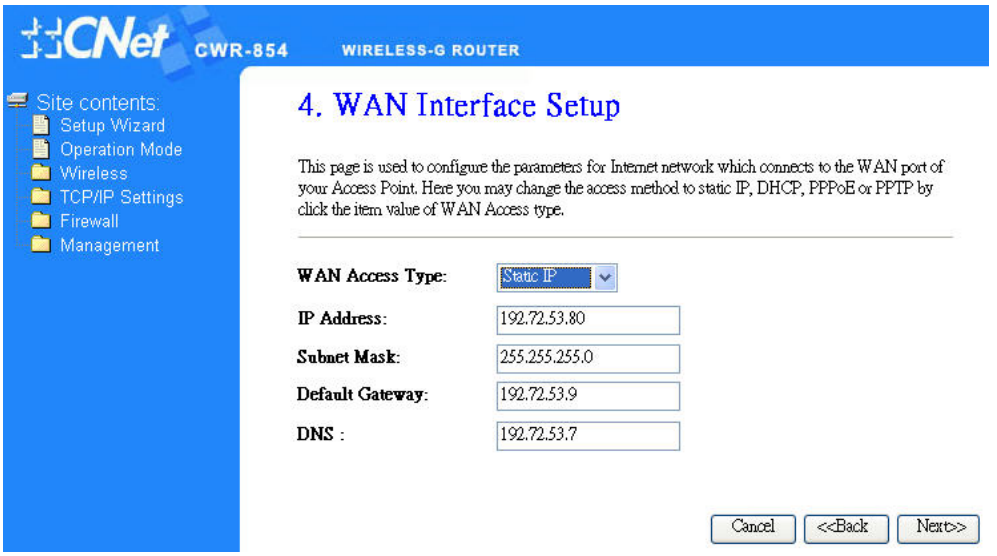
- ✓ **IP Address**: Current IP address of the Wireless-G Router, not WAN IP address.
- ✓ **Subnet Mask**: Current subnet mask for the Wireless-G Router, not WAN subnet mask address
- ✓ **Cancel**: To skip the current settings and jump to the **Setup Wizard** page.
- ✓ **Back**: To skip the current settings and go back to the last page.
- ✓ **Next:** Go to the next page.

After typing in the IP Address and Subnet Mask, click "**Next**" to move on the WAN interface setup page.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.1.4 WAN Interface Setup

In this screen users must identify and configure the connection type used for connecting to their Internet Service Provider (ISP).



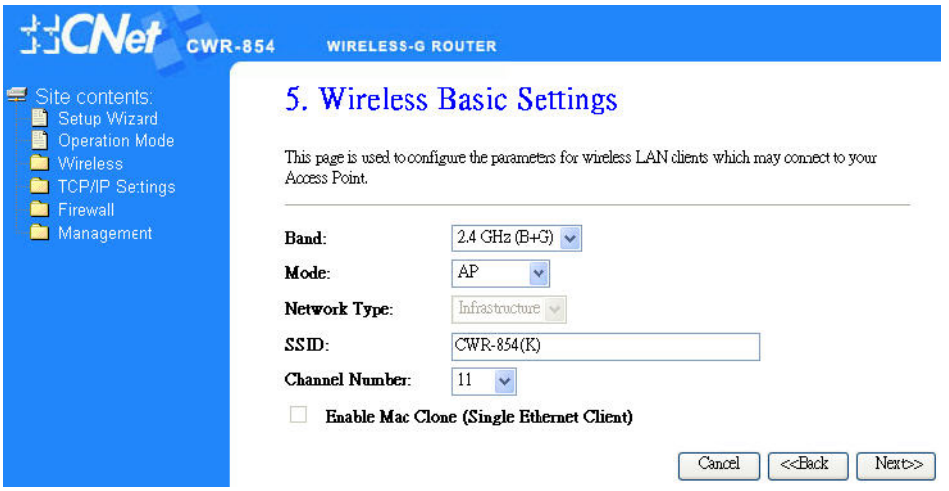
- ✓ **WAN Access Type**: CWR supports 4 kinds of access type to connect the ISP – Static IP, DHCP Client, PPPoE, PPTP.
- ✓ **Cancel**: To skip the current settings and jump to the **Setup Wizard** page.
- ✓ **Back**: To skip the current settings and go back to the last page.
- ✓ **Next:** Go to the next page.

After all items are set, click "**Next**" to advance to the next screen, Wireless Basic Settings page.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.1.5 Wireless Basic Settings

In the Wireless Basic Settings page, users can configure the operating “Band” and “Mode” as well as “Network Type”, ” SSID”, “Channel Number” and if required MAC address cloning.



- ✓ **Operating Band**: 802.11B/G, 802.11G or 802.11B
- ✓ **Operating Mode**: AP, Client, WDS and AP+WDS.
- ✓ **Network type**: when operating mode is “Client” mode, users can select the network type as “infrastructure” or “Ad-hoc”.
- ✓ **SSID**: The SSID differentiates one WLAN from another, therefore, all wireless access points/routers and all wireless devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters
- ✓ **Channel Number**: The number of channels supported depends on the region this Wireless-G Router is used in. All stations communicating with this Wireless-G Router must use the same channel. **(Note: not supported in client mode)**
- ✓ **Enable Mac clone**: when operating mode is “Client” and only one Ethernet client exists, users can enable the Mac clone feature to easily connect to the wireless station.
- ✓ **Cancel**: To skip the current settings and jump to the **Setup Wizard** page.
- ✓ **Next**: Go to the next page.
- ✓ **Back**: To skip the current settings and go back to the last page.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.1.6 Wireless Security Setup

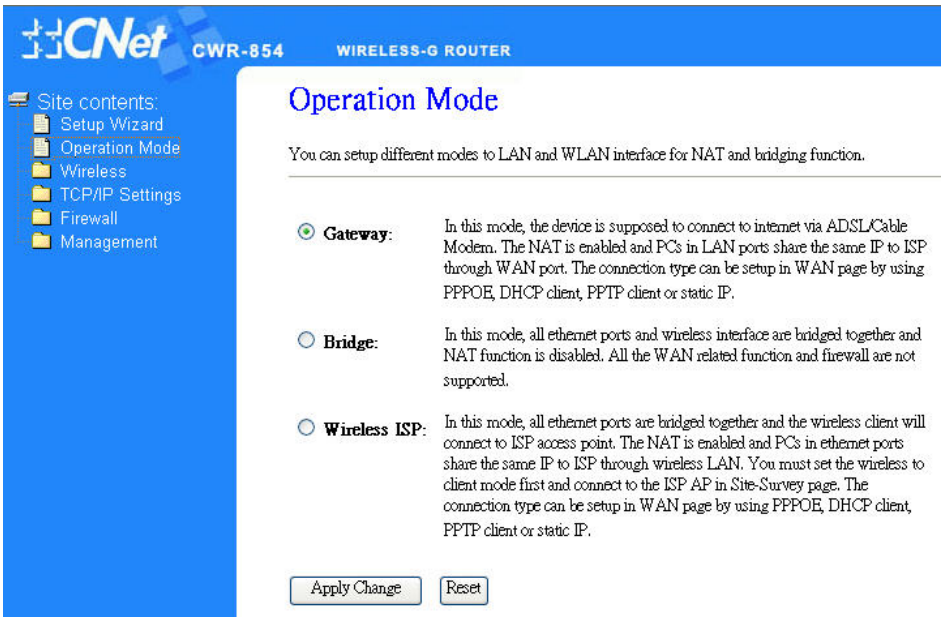
This page is used to configure wireless security. CWR-854 could support WEP, WPA and WPA2 Encryption key. Those encryption methods could prevent any unauthorized access to your wireless network.

After all items are set, click on "**Finished**" button to save all the parameters you have set, and the router will reboot automatically.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.2 Operation Mode

This page is used to configure which mode wireless broadband router acts.


CNet
CWR-854
WIRELESS-G ROUTER
Site contents:
Setup Wizard
Operation Mode
Wireless
TCP/IP Settings
Firewall
Management
Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Bridge:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
Apply Change
Reset

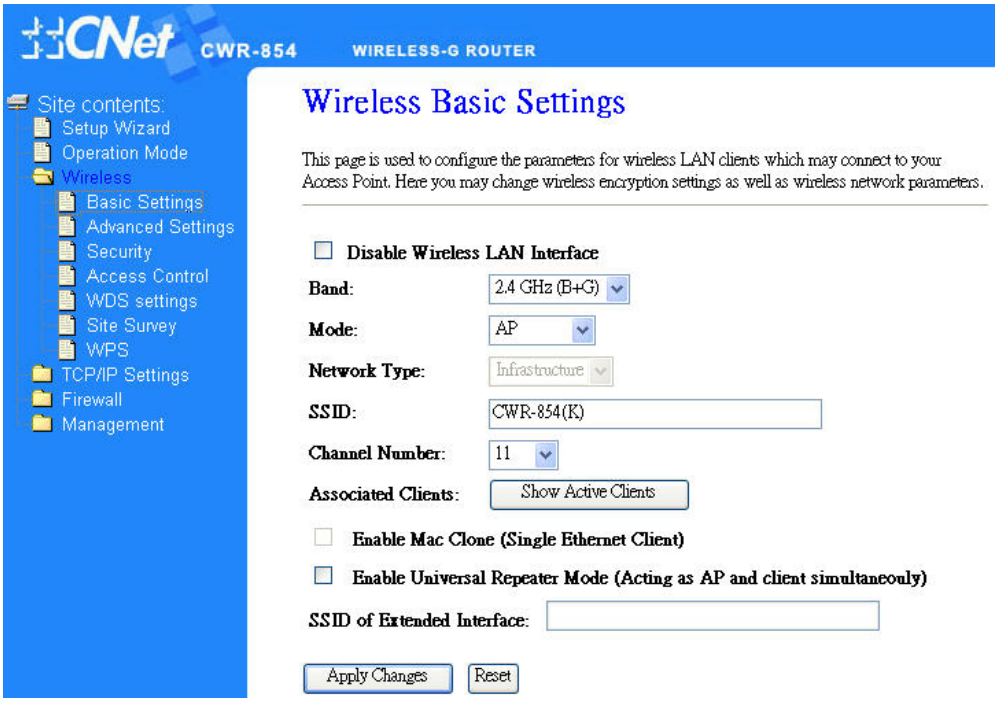
- ✓ **Gateway**: Traditional gateway configuration. It always connects to the Internet via ADSL/Cable Modem. LAN interface, WAN interface, Wireless interface, NAT and Firewall modules are applied to this mode
- ✓ **Bridge**: Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported
- ✓ **Wireless ISP**: Switch Wireless interface to be switched to the WAN port and all Ethernet ports in bridge mode.
- ✓ **Apply Changes**: Click the Apply Changes button to complete the new configuration setting.
- ✓ **Reset:** Click the Reset button to abort change and recover the previous configuration setting.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3 Wireless

3.3.1 Basic Settings

The Wireless Basic Settings include Band, Mode, SSID, Channel Number and other wireless settings.



- ✓ **Disable Wireless LAN Interface**: The wireless interface will be disabled when checked.
- ✓ **Band**: This Wireless-G Router can support three RF band: 802.11B/G, 802.11G and 802.11B.
- ✓ **Mode**: This Wireless-G Router supports four operating modes: AP, client, WDS, and AP+WDS.
- ✓ **Network Type**: In Client mode, users can select the network type as “Infrastructure” or “Ad-hoc”. Infrastructure mode allows the PCs or small LAN able to access the network via the Access Point. Ad-hoc mode is a station alone with other wireless station and can establish a small wireless network with connect to an Access Point.
- ✓ **SSID**: The SSID differentiates one WLAN from another, therefore, all wireless access points/routers and all wireless devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters.
- ✓ **Channel Number**: The number of channels supported depends on the region Wireless-G Router is used in. All stations communicating with this Wireless-G Router must be on the same channel.
- ✓ **Associated Clients**: When clicked on “Show Active Client” button, all associated wireless clients will be shown. The feature is only available in AP and AP+WDS modes.
- ✓ **Enable Mac clone**: When operating mode is Client mode and only one Ethernet client exists, users can enable this Mac clone feature to connect with wireless station easily.
- ✓ **Enable Universal Repeater Mode**: The router can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.
- ✓ **SSID for Extended Interface:** The SSID could be defined for the wireless LAN

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

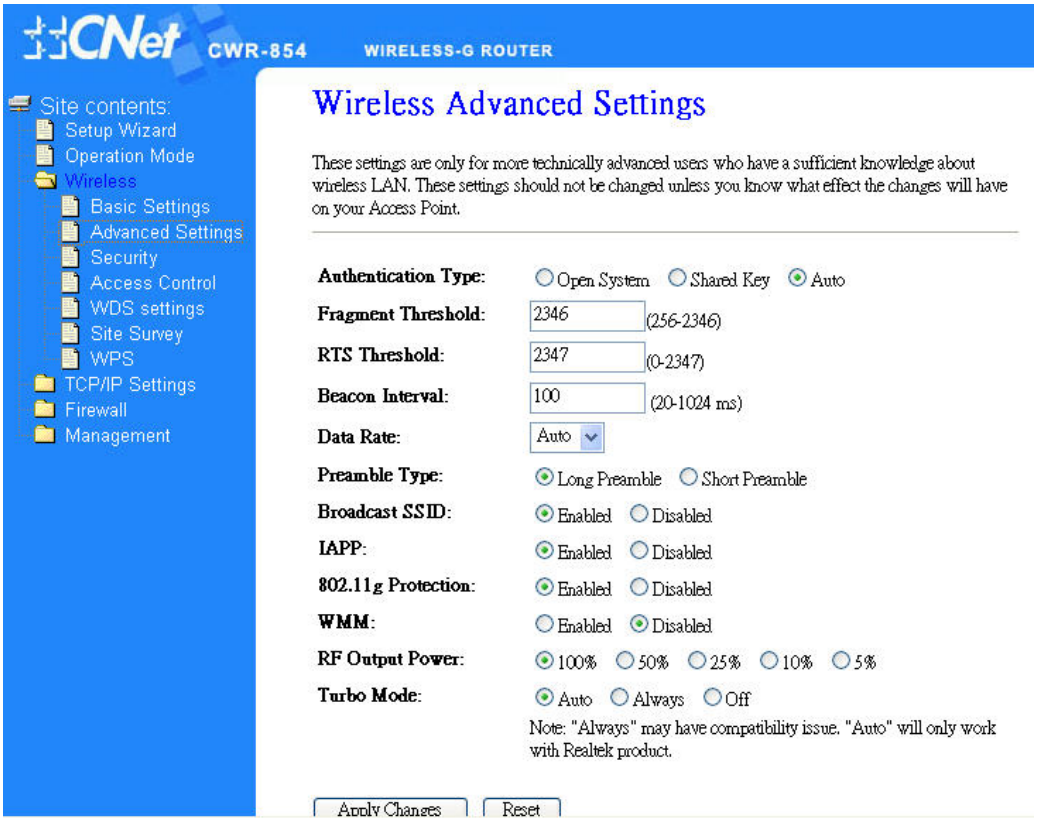
user when the router connect to a Root AP (When Universal Repeater Mode be enabled)

- ✓ **Apply Changes**: Click on “Apply Changes” to save changes and logout.
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3.2 Wireless Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable.


CNet
CWR-854
WIRELESS-G ROUTER
Site contents:
Setup Wizard
Operation Mode
Wireless
Basic Settings
Advanced Settings
Security
Access Control
WDS settings
Site Survey
WPS
TCP/IP Settings
Firewall
Management
Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Authentication Type: Open System Shared Key Auto
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Data Rate: Auto
Preamble Type: Long Preamble Short Preamble
Broadcast SSID: Enabled Disabled
IAPP: Enabled Disabled
802.11g Protection: Enabled Disabled
WMM: Enabled Disabled
RF Output Power: 100% 50% 25% 10% 5%
Turbo Mode: Auto Always Off
Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.
Apply Changes
Reset

- ✓ **Authentication Type**: The router supports three kinds of the authentication types- Open System, Shared Key, and Auto.
- ✓ **Fragment Threshold**: Fragmentation mechanism is used for improving the efficiency when traffic is high in the wireless network. If a wireless client often transmits large files, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346.
- ✓ **RTS Threshold**: RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. "Hidden Node" is a situation in which two stations are within range of the same wireless access point/router, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Wireless-G Router, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when simultaneously arriving at the Wireless-G Router. The collision will most certainly result in loss of messages of both stations. If the "Hidden Node" problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. The default value is 2347.
- ✓ **Beacon Interval:** Beacon interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the wireless router).
- ✓ **Data Rate**: By default, it selects the highest rate for transmission.
- ✓ **Preamble Type**: A preamble is a signal used in wireless environments to synchronize transmit timings including Synchronization and Start Frame Delimiter. In a "noisy" network environment, Preamble Type should be set to Long. The Short Preamble is intended for applications where minimum overhead and

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

maximum performance is desired.

- ✓ **Broadcast SSID**: When enabled allows all wireless stations to detect the SSID of this wireless router.
- ✓ **IAPP**: The Inter-Access Point Protocol (IAPP) can extend multi-vendor interoperability to the roaming function.
- ✓ **802.11g Protection**: Is used to prevent packet collision and increase performance in wireless networks with both 802.11b (using CCK modulation) and 802.11g (using OFDM modulation) devices.
- ✓ **WMM**: The short of Wi-Fi Multi-Media. It will enhance the data transfer performance of multimedia content when they are being transferred over wireless network. If you do not know what it is / not sure if you need it. It's safe to set this option to "Enable", however, default value is "Disable".
- ✓ **RF Output Power**: Output power can be set of wireless radio. Unless you are using this wireless router in a really big space. You may not have to set output power to 100%. This will enhance security.
- ✓ **Turbo Mode**: The data rate will up to 72Mbps when the turbo mode is enabled. Please be noted the turbo mode might have compatibility issue when be used without Realtek solution.
- ✓ **Apply Changes**: Click on "Apply Changes" to save the setting.
- ✓ **Reset:** Click on "Reset" button to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3.3 Security

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link**. There are five Encryption types supported: “None”, “WEP”, “WPA (TKIP)”, ”WPA2(AES)”, and “WPA2 Mixed”.

□ ***No Encryption Used***

- ✓ **Encryption: “None”** means no encryption used. Users can enable 802.1x Authentication and enter the RADIUS server parameters – port, IP address and Password.
- ✓ **Use 802.1x Authentication**: Is a port access protocol for protecting networks via authentication. If wireless user is authenticated (via 802.1x), a virtual port is opened on the router/access point allowing for communication. If authentication fails, the router/access point will deny access to the user.
- ✓ **Authentication RADIUS Server:** RADIUS is the Remote Access Dial-In User Service, an Authorization, Authentication, and Accounting (AAA) client-server protocol, which is used when a AAA dial-up client logs in or out of a Network Access Server. Typically, a RADIUS server is used by Internet Service Providers (ISP) to perform AAA tasks. AAA phases are described as follows:
  - ■ Authentication phase: Verifies a user name and password against a local database. After the credentials are verified, the authorization process begins.
  - ■ Authorization phase: Determines whether a request is allowed access to a resource. An IP address is assigned for the Dial-Up client.
  - ■ Accounting phase: Collects information on resource usage for the purpose of trend analysis, auditing, session time billing, or cost allocation.

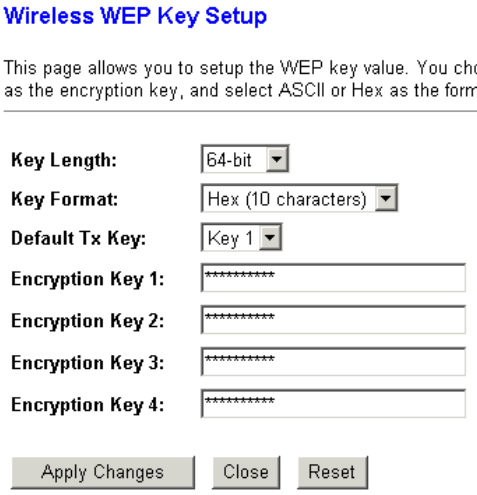
  Users must enter RADIUS Server’s **Port** number, **IP address** and **Password**.
- ✓ **Apply Changes**: Click on “Apply Changes” to save the setting.
- ✓ **Reset:** Click on “Reset” button to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

□ ***WEP Encryption***

- ✓ **Encryption:** "**WEP**" (Wired Equivalent Privacy) encryption type.
- ✓ **Set WEP Key:** Only active when "**Use 802.1x Authentication**" is not selected.
- ✓ **Use 802.1x Authentication**: When this feature is enabled, users need to enter parameters of the "**RADIUS Server**" and select the encryption key length to be "**WEP 64bits**" or "**WEP 128bits**".
- ✓ **Authentication RADIUS Server:** RADIUS Server's **Port** number, **IP address** and **Password.**
- ✓ **Apply Changes**: Click on "Apply Changes" to save the setting.
- ✓ **Reset:** Click on "Reset" button to undo your changes.

When "Set WEP Key" is selected, the **Wireless WEP Key Setup** window will display as below:


Wireless WEP Key Setup
This page allows you to setup the WEP key value. You choose either 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.
Key Length: 64-bit
Key Format: Hex (10 characters)
Default Tx Key: Key 1
Encryption Key 1: **********
Encryption Key 2: **********
Encryption Key 3: **********
Encryption Key 4: **********
Apply Changes
Close
Reset

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

- **Key Length**: Choose either 64-bit or 128-bit.
- **Key Format**: Select Hexadecimal or ASCII .
- **Default Tx Key**: Select the default encryption Key (Key1 to Key4) being transmitted.
- **Encryption Key 1**: enter any key code for Encryption Key 1.
- **Encryption Key 2**: enter any key code for Encryption Key 2.
- **Encryption Key 3**: enter any key code for Encryption Key 3.
- **Encryption Key 4**: enter any key code for Encryption Key 4.
- **Apply Changes**: Click on “Apply Changes” to save settings.
- **Close**: To close this window.
- **Reset:** Click on “Reset” button to undo your changes.
- **Help**: To request help information.

WEP encryption key (secret key) length:

Format	Length	
	64-bit	128-bit
ASCII	5 characters	13 characters
HEX	10 hexadecimal codes	26 hexadecimal codes

□ ***WPA / WPA2 Encryption***

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

- **Encryption: "WPA"** stands for Wi-Fi Protected Access. There are three encryption modes – **TKIP**, **AES** and **Mixed**.
  - **TKIP**: Temporal Key Integrity Protocol.
  - **AES**: Advanced Encryption Standard.
  - **Mixed**: WPA2 Mixed mode operation permits the coexistence of WPA and WPA2 clients on a common SSID. WPA2 Mixed Mode is a Wi-Fi Certified feature. During WPA2 Mixed Mode, the Wireless-G Router advertises the encryption ciphers (TKIP, CCMP, other) that are available for use. The client selects the encryption cipher it likes to use and the selected cipher is used for encryption between the client and Wireless-G Router.

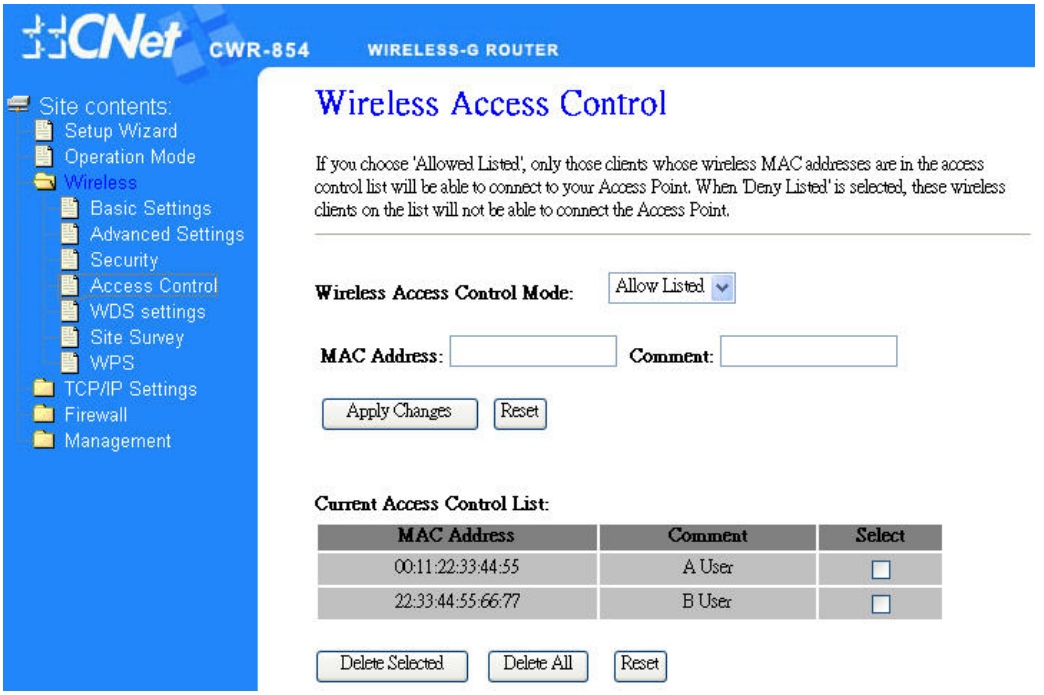
Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

- ✓ **WPA Authentication Mode**: There are two modes of WPA authentication - **Enterprise (RADIUS)** and **Personal (Pre-Shared Key)**.
- ✓ **WPA Cipher Suite**: There are two modes could be chose – TKIP and AES (
- ✓ **WPA2 Cipher Suite**: There are two method could be chose – TKIP and AES
- ✓ **RADIUS Server**: When user chooses RADIUS authentication, there are three parameters for the RADIUS server to be set – Port, IP address and Password.
- ✓ **Pre-Shared Key**: When user chooses Pre-Shared Key authentication, there are two types of input format – ASCII and Hex.
- ✓ **Enable Pre-Authentication**: Only valid when WPA2(AES) and WPA2 (Mixed mode) encryption is selected. When user chooses **Enterprise (RADIUS)** authentication, this feature allows the radius server to do the pre-authentication process.
- ✓ **Apply Changes**: Click on “Apply Changes” to save the settings.
- ✓ **Reset:** Click on “Reset” button to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3.4 Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on "Apply Changes" to save the new addition. To delete a MAC address, select its corresponding checkbox under the **Select** column and click on "Delete Selected" button.



- ✓ **Wireless Access Control Mode**: There are three types of access control options:
  - ■ **Disable**
  - ■ **Allow Listed**: When selected, only clients whose wireless MAC addresses are in the access control list will be able to connect to the Wireless-G Router.
  - ■ **Deny Listed**: When selected, wireless clients on the list are blocked from accessing the Wireless-G Router.
- ✓ **MAC Address**: This field is used to enter the client's MAC address.
- ✓ **Comment:** This field is used for adding any comments.
- ✓ **Apply Changes** : This button is used to apply new settings.
- ✓ **Delete Selected** : This button is used to delete a selected client.
- ✓ **Delete All**: To delete all clients in the **Current Access Control List**.
- ✓ **Reset**: To undo all changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3.5 WDS Settings

When selected in the Basic Settings page and enabled here, Wireless Distribution System (WDS) enables the router to be used as a wireless bridge. Two Wireless-G Routers in bridge mode can communicate with each other through their wireless interfaces. To accomplish this, all wireless routers should be set to the same channel and the MAC address of other AP / Routers should be entered in the table.

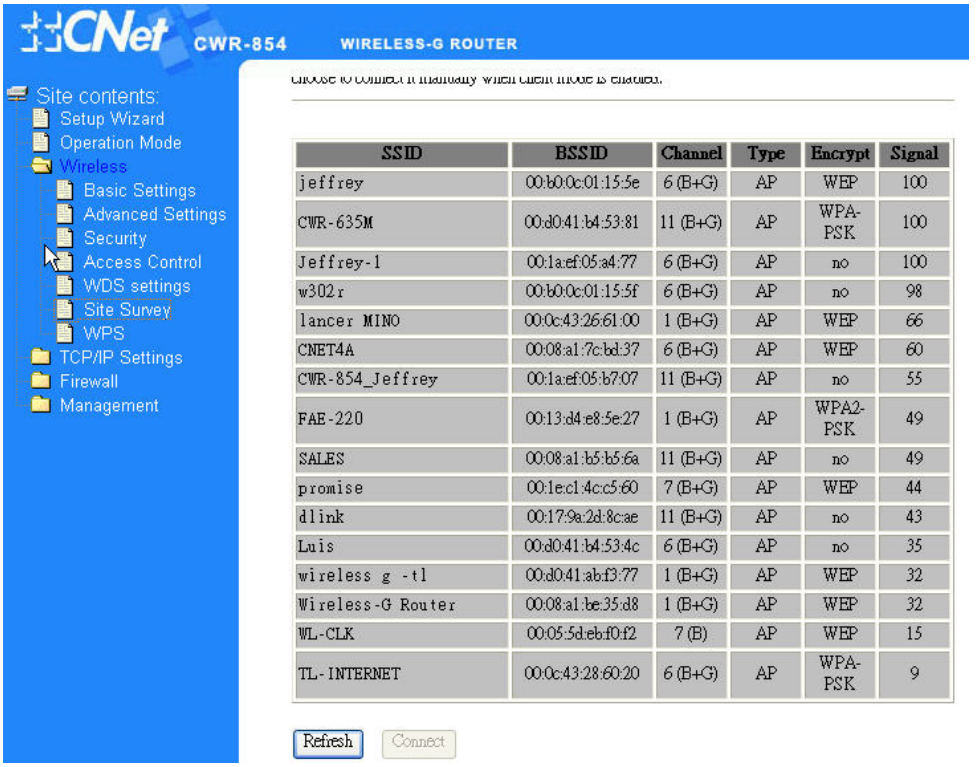
- ✓ **Enable WDS**: enable WDS function.
- ✓ **Add WDS AP**: Fill in the other AP/router's MAC address what you want to bridge.
- ✓ **Comment:** This field is used for adding any comments.
- ✓ **Apply Changes:** This button is used to apply new settings
- ✓ **Reset:** To undo all changes.
- ✓ **Set Security**: To setup wireless security for WDS.
- ✓ **Show Statistics**: Shows the MAC address, transmission and reception packet counters for each configured WDS AP.
- ✓ **Current WDS AP List**: A table showing current WDS AP's.
- ✓ **Delete Selected**: Delete the selected WDS AP.
- ✓ **Delete All**: Delete all the WDS APs.
- ✓ **Reset:** Click on "Reset" to undo changes.

Notes: Please set the wireless mode to "WDS" or "AP+WDS" first. (Wireless → Basic Setting)

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3.6 Site Survey

The Wireless Site Survey tool will scan and display all available wireless networks. Click on "**Refresh**" to search/re-scan for available Wireless-G Router(s) or IBSS(s). If any Wireless-G Router or IBSS is found, select and click on connect to start a connection.



SSID	BSSID	Channel	Type	Encrypt	Signal
jeffrey	00:b0:0c:01:15:5e	6 (B+G)	AP	WEP	100
CWR-635M	00:d0:41:b4:53:81	11 (B+G)	AP	WPA-PSK	100
Jeffrey-1	00:1a:ef:05:a4:77	6 (B+G)	AP	no	100
w302r	00:b0:0c:01:15:5f	6 (B+G)	AP	no	98
lancer MINO	00:0c:43:26:61:00	1 (B+G)	AP	WEP	66
CNET4A	00:08:a1:7c:bd:37	6 (B+G)	AP	WEP	60
CWR-854_Jeffrey	00:1a:ef:05:b7:07	11 (B+G)	AP	no	55
FAE-220	00:13:d4:e8:5e:27	1 (B+G)	AP	WPA2-PSK	49
SALES	00:08:a1:b5:b5:6a	11 (B+G)	AP	no	49
promise	00:1e:c1:4c:c5:60	7 (B+G)	AP	WEP	44
dlink	00:17:9a:2d:8c:ae	11 (B+G)	AP	no	43
Luis	00:d0:41:b4:53:4c	6 (B+G)	AP	no	35
wireless g -tl	00:d0:41:ab:f3:77	1 (B+G)	AP	WEP	32
Wireless-G Router	00:08:a1:be:35:d8	1 (B+G)	AP	WEP	32
WL-CLK	00:05:5d:eb:f0:f2	7 (B)	AP	WEP	15
TL-INTERNET	00:0c:43:28:60:20	6 (B+G)	AP	WPA-PSK	9

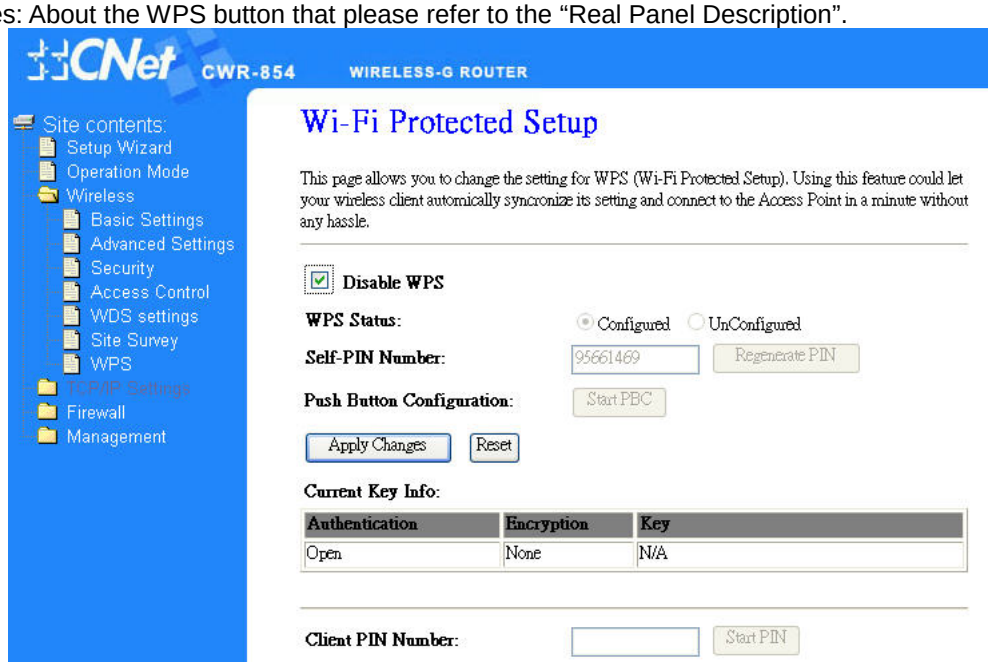
- ✓ **Refresh:** Click on "**Refresh**" button to renew and show the table.
- ✓ **Connect:** You can select any listed wireless network and then click on "**Connect**" button, to establish a connection.
- ✓ **Help**: To request help information.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.3.7 WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize it's setting and connect to the Access Point in a minute without any hassle. CWR-854 could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.

Notes: About the WPS button that please refer to the "Real Panel Description".



- ✓ **Disable WPS:** WPS will be disabled when clicked
- ✓ **WPS Status:** Show WPS status is Configured or Unconfigured.
- ✓ **Self-PIN Number:** Fill in the PIN Number of AP to register the wireless distribution system access capacity**.**
- ✓ **Push Button Configuration:** The **Start PBC** button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could connect it automatically when client join PBC mode.
- ✓ **Apply Changes:** Click the **Apply Changes** button to complete the new configuration setting.
- ✓ **Reset:** Click the **Reset** button to abort change and recover the previous configuration setting.
- ✓ **Current Key Info:**
  - Authentication: It shows the Authentication is opened or closed.
  - Encryption: It shows the Encryption mode.
  - Key: It shows the Encryption key.
- ✓ **Client PIN Number:** Fill in the **Client PIN Number** from your Client sites.

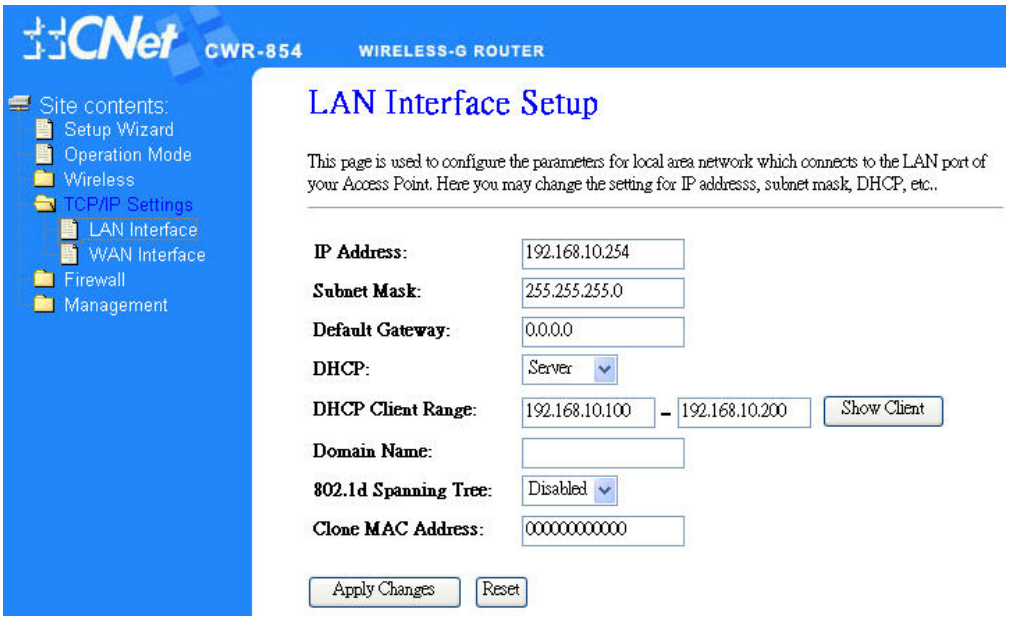
Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.4 TCP / IP Settings

Please follow the following instruction to build the network connection between the wireless router and your computers or network devices.

3.4.1 LAN Interface

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Broadband Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.



- ✓ **IP Address:** Fill in the IP address of LAN interfaces of this WLAN Access Point.
- ✓ **Subnet Mask:** Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
- ✓ **Default Gateway:** Fill in the default gateway for LAN interfaces out going data packets.
- ✓ **DHCP:** Click to select **Disabled, Client** or **Server** in different operation mode of wireless Access Point.
- ✓ **DHCP Client Range:** Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
- ✓ **Show Client:** Click to open the **Active DHCP Client Table** window that shows the active clients with their assigned IP address, MAC address and time expired information. **[Server mode only]**
- ✓ **Static DHCP:** Select enable or disable the Static DHCP function from pull-down menu. **[Server mode only]**
- ✓ **Set Static DHCP:** Manual setup Static DHCP IP address for specific MAC address. **[Server mode only]**
- ✓ **Domain Name:** Assign Domain Name and dispatch to DHCP clients. It is optional field.
- ✓ **802.1d Spanning Tree:** Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
- ✓ **Clone MAC Address:** Fill in the MAC address that is the MAC address to be cloned.
- ✓ **Apply Changes:** Click the **Apply Changes** button to complete the new

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

configuration setting.

- ✓ **Reset:** Click the **Reset** button to abort change and recover the previous configuration setting.

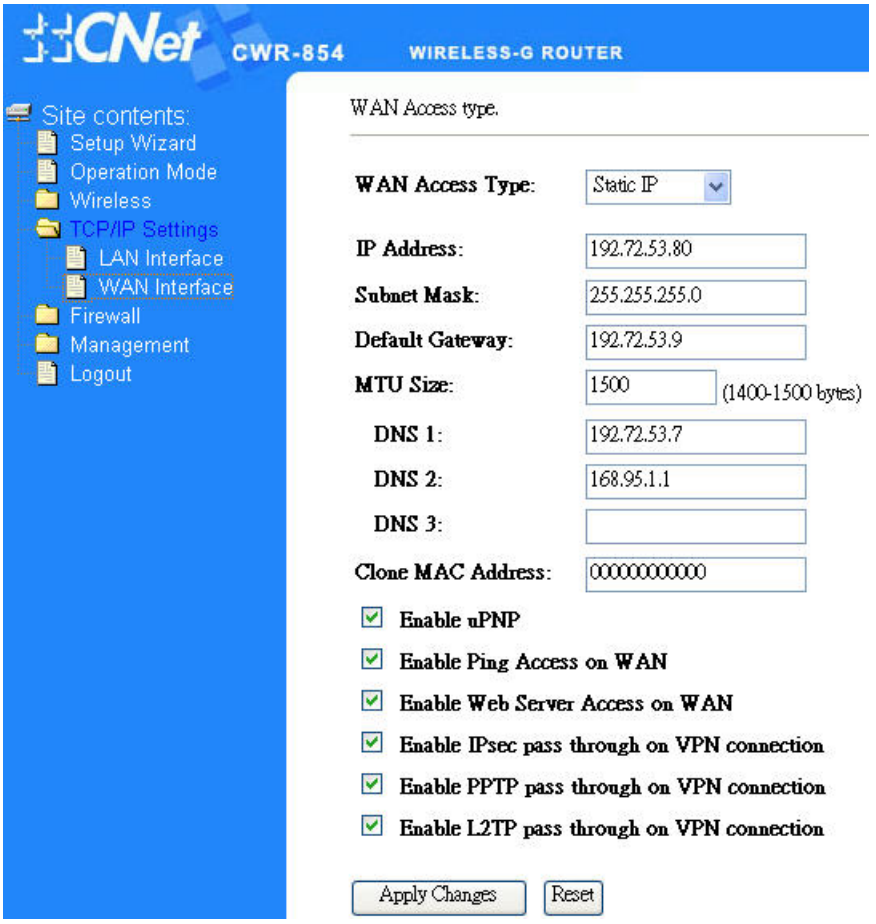
Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.4.2 WAN Interface

"WAN Interface Setup" allows users to select the WAN connection type and configure the parameters pertaining to the WAN interface. The four different access types supported on this router are: Static IP, DHCP Client, PPPoE and PPTP.

□ **Static IP**

This is the connection type used when users have a fixed IP address from their ISP. In this case the IP address, Subnet Mask, Default Gateway, Primary and Secondary DNS Server IPs should be acquired from the ISP.



- ✓ **WAN Access Type**: **Static IP** is the connection type selected.
- ✓ **IP Address**: This is the fixed IP address received from ISP.
- ✓ **Subnet Mask**: Subnet mask provided by ISP.
- ✓ **Default Gateway**: Default gateway provided by ISP.
- ✓ **MTU Size**: Fill in the MTU size of MTU Size. The default value is 1400.
- ✓ **DNS1**: Primary DNS provided by your ISP.
- ✓ **DNS2**: Secondary DNS if necessary.
- ✓ **DNS3**: This Tertiary DNS if necessary.
- ✓ **Clone MAC Address**: Some ISPs use the MAC address of a network card for authentication, users may use "Clone MAC Address to" duplicate the MAC address to the MAC address in the WAN port.
- ✓ **Enable UPnP**: It allows enabling or disabling uPNP feature. If enabled, all client systems that support uPNP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration.
- ✓ **Enable Ping Access on WAN**: Click the checkbox to enable WAN ICMP

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

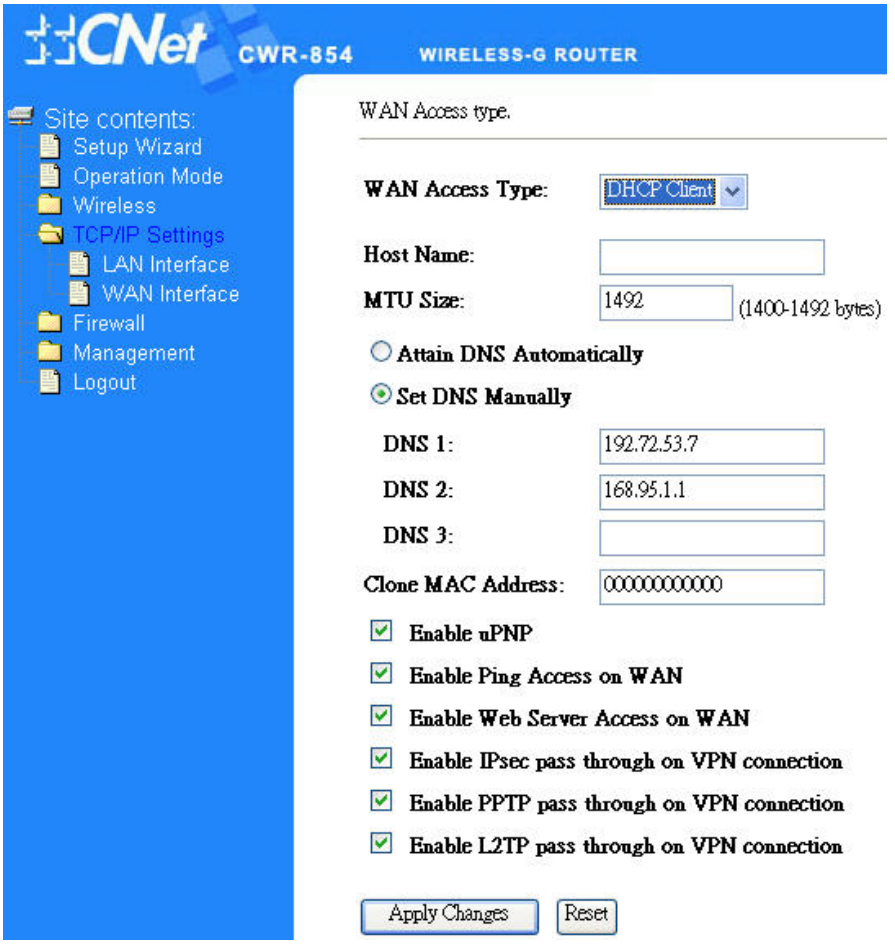
response.

- ✓ **Enable Web Server Access on WAN**: Click the checkbox to enable web configuration from WAN side.
- ✓ **Enable IPSec pass through on VPN connection**: Click the checkbox to enable IPSec packet pass through.
- ✓ **Enable PPTP pass through on VPN connection**: Click the checkbox to enable PPTP packet pass through.
- ✓ **Enable L2TP pass through on VPN connection**: Click the checkbox to enable L2TP packet pass through.
- ✓ **Apply Changes**: Click on “Apply Changes” to save changes and logout.
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

□ DHCP Client

The DHCP client also called "Dynamic IP address" is the mostly used connection type by cable broadband service providers. In this case the user will automatically receive all IP information from the service provider.



- ✓ **WAN Access Type**: **DHCP Client** connection type.
- ✓ **Host Name**: Fill in the host name of Host Name. The default value is empty.
- ✓ **MTU Size**: Fill in the MTU size of MTU Size. The default value is 1400.
- ✓ **Attain DNS Automatically**: Click to select getting DNS address for **DHCP** support.
- ✓ Please select **Set DNS Manually** if the **DHCP** support is selected.
- ✓ **DNS1**: Primary DNS IP address.
- ✓ **DNS2**: Secondary DNS if necessary.
- ✓ **DNS3**: Tertiary DNS if necessary.
- ✓ **Clone MAC Address**: Some ISPs use the MAC address of a network card for authentication, users may use “Clone MAC Address to” duplicate the MAC address to the MAC address in the WAN port.
- ✓ **Enable UPnP**: It allows enabling or disabling uPNP feature. If enabled,, all client systems that support uPNP, like Windows XP, can discover this router automatically and access the Internet through this router without any

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

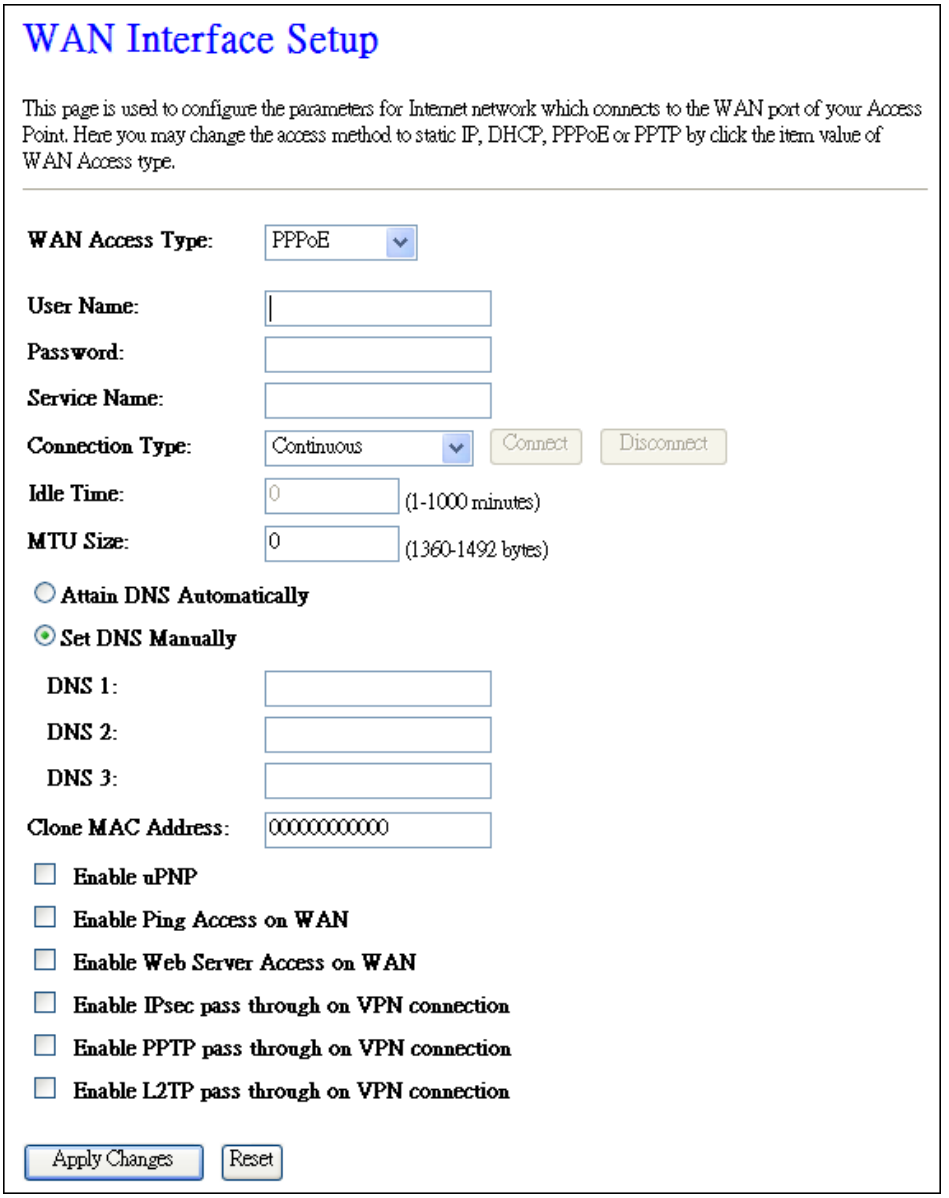
configuration.

- ✓ **Enable Ping Access on WAN**: Click the checkbox to enable WAN ICMP response.
- ✓ **Enable Web Server Access on WAN**: Click the checkbox to enable web configuration from WAN side.
- ✓ **Enable IPSec pass through on VPN connection**: Click the checkbox to enable IPSec packet pass through.
- ✓ **Enable PPTP pass through on VPN connection**: Click the checkbox to enable PPTP packet pass through.
- ✓ **Enable L2TP pass through on VPN connection**: Click the checkbox to enable L2TP packet pass through.
- ✓ **Apply Changes**: Click on “Apply Changes” to save changes and logout.
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

□ **PPPoE**

PPPoE stands for “Point-to-Point Protocol over Ethernet”. PPP is the technology used for dialup Internet access. PPPoE works similarly except it works over a network connection. In this connection type, users are required to enter their PPPoE username and password. Some ISPs also require a service name to be entered. Usually, it’s not needed to enter the IP/DNS addresses. However, if users have static IPs through PPPoE, then they will need to enter IP and DNS addresses ISP provides.



- ✓ **WAN Access Type**: **PPPoE** connection type.
- ✓ **User Name**: User Name provided by ISP.
- ✓ **Password**: Password provided by ISP.
- ✓ **Service Name**: Fill in the service name of Service Name. The default value is empty.
- ✓ **Connection Type**: There are three connection types – **continuous**, **connect on demand** and **manual**.
  - ■ **Continuous**: the connection to the ISP is always connected.
  - ■ **Connect On Demand**: the connection to the ISP is initialized only when an

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

application is active to connect the Internet.

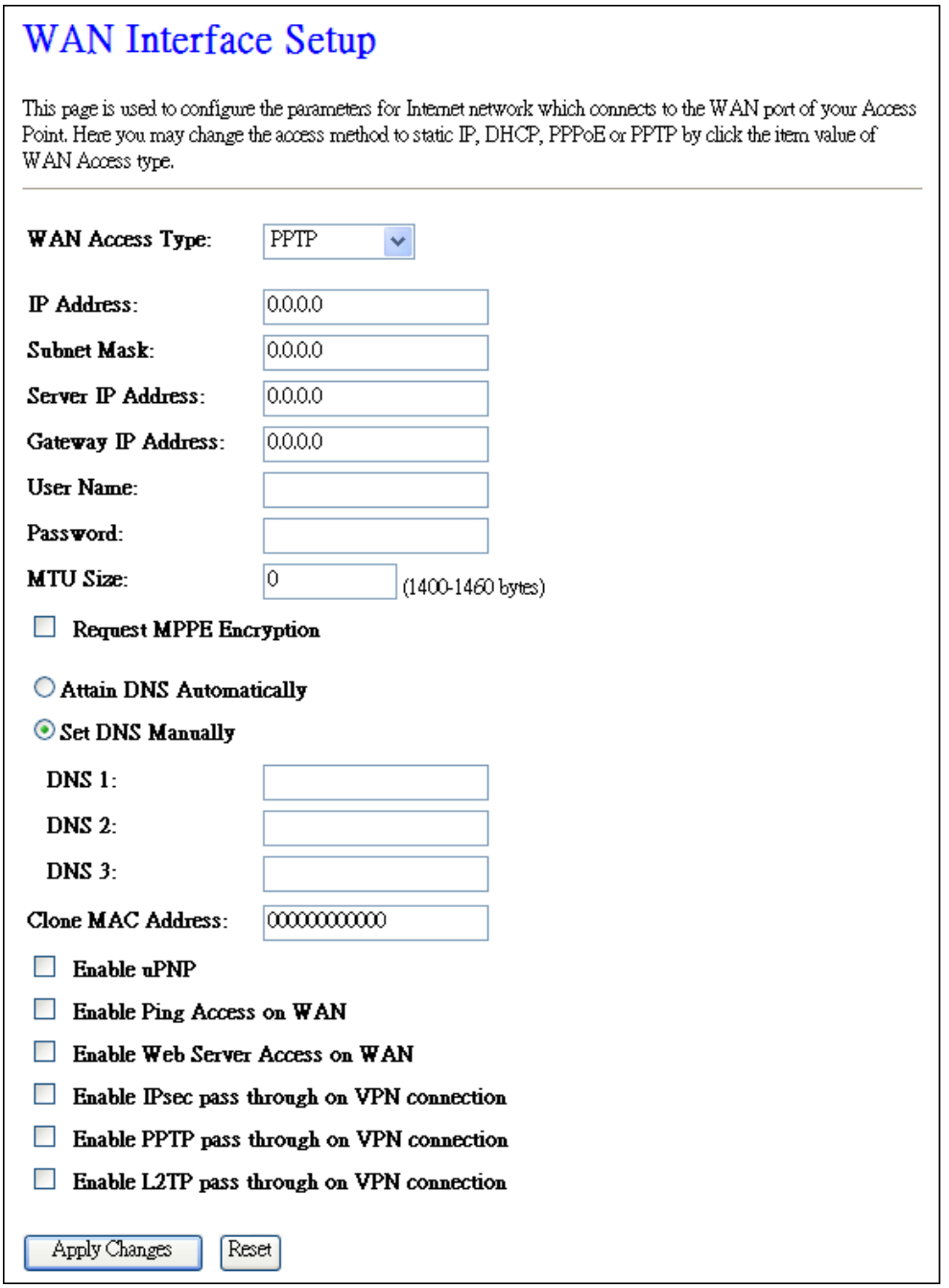
- **Manual**: the connection to the ISP is set manually.

- ✓ **Idle Time**: Only active only when **Connect On Demand** is selected. This is the time it takes for the router to disconnect from the ISP if no access request is received.
- ✓ **MTU Size**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1452, to have the router select the best MTU for your Internet connection.
- ✓ **Attain DNS Automatically**: When enabled DNS is obtained automatically.
- ✓ **Set DNS Manually**: allow user to set the DNS manually.
- ✓ **DNS1**: Primary DNS IP address.
- ✓ **DNS2**: Secondary DNS if necessary.
- ✓ **DNS3**: Tertiary DNS if necessary.
- ✓ **Clone MAC Address**: Some ISPs use the MAC address of a network card for authentication, users may use “Clone MAC Address to” duplicate the MAC address to the MAC address in the WAN port..
- ✓ **Enable uPNP**: It allows enabling or disabling uPNP feature. If enabled,, all client systems that support uPNP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration.
- ✓ **Enable Ping Access on WAN**: Click the checkbox to enable WAN ICMP response.
- ✓ **Enable Web Server Access on WAN**: Click the checkbox to enable web configuration from WAN side.
- ✓ **Enable IPSec pass through on VPN connection**: Click the checkbox to enable IPSec packet pass through.
- ✓ **Enable PPTP pass through on VPN connection**: Click the checkbox to enable PPTP packet pass through.
- ✓ **Enable L2TP pass through on VPN connection**: Click the checkbox to enable L2TP packet pass through.
- ✓ **Apply Changes**: Click on “Apply Changes” to save changes and logout.
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

□ PPTP

PPTP stands for “Point-to-Point Tunneling Protocol”. PPTP is used to join 2 networks using the Internet as an intermediary network. It allows you to connect your home and work network over the Internet. The key is to enter the PPPTP userID, password, and PPTP Gateway IP address. The IP addresses, subnet mask, and default gateway may or may not be required.



- ✓ **WAN Access Type**: **PPTP** connection type.
- ✓ **IP Address**: IP Address provided by ISP.
- ✓ **Subnet Mask**: Subnet Mask provided by ISP.
- ✓ **Server IP Address**: Server IP Address provided by ISP.
- ✓ **Gateway IP Address**: Fill in the gateway for WAN interface out going data packets.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

- ✓ **User Name**: User Name provided by ISP.
- ✓ **Password**: Password provided by ISP
- ✓ **MTU Size**: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, 1452, to have the router select the best MTU for your Internet connection.
- ✓ **Request MPPE Encryption**: Click the checkbox to enable request MPPE encryption.
- ✓ **Attain DNS Automatically**: When enabled DNS is obtained automatically.
- ✓ **Set DNS Manually**: allow user to set the DNS manually.
- ✓ **DNS1**: Primary DNS IP address.
- ✓ **DNS2**: Secondary DNS if necessary.
- ✓ **DNS3**: Tertiary DNS if necessary.
- ✓ **Clone MAC Address**: Some ISPs use the MAC address of a network card for authentication, users may use "Clone MAC Address to" duplicate the MAC address to the MAC address in the WAN port.
- ✓ **Enable uPNP**: It allows enabling or disabling uPNP feature. If enabled,, all client systems that support uPNP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration.
- ✓ **Enable Ping Access on WAN**: Click the checkbox to enable WAN ICMP response.
- ✓ **Enable Web Server Access on WAN**: Click the checkbox to enable web configuration from WAN side.
- ✓ **Enable IPSec pass through on VPN connection**: Click the checkbox to enable IPSec packet pass through.
- ✓ **Enable PPTP pass through on VPN connection**: Click the checkbox to enable PPTP packet pass through.
- ✓ **Enable L2TP pass through on VPN connection**: Click the checkbox to enable L2TP packet pass through.
- ✓ **Apply Changes**: Click on "Apply Changes" to save changes and logout.
- ✓ **Reset:** Click on "Reset" to undo your changes.

Notes: PPTP Gateway. Your ISP will provide you with the Gateway IP Address. If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have PPTP gateway then enter the ISP's Gateway IP address above.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.5 Firewall

3.5.1 Port Filtering

When enabled packets are denied access to Internet/filtered based on their port address.

- ✓ **Enable Port Filtering**: Enable the Port Filtering function.
- ✓ **Port Range**: Enter the Port range (1 to 65535) that are to be blocked..
- ✓ **Protocol**: Protocols to be blocked UDP, TCP or both.
- ✓ **Comment**: Allow user to add any comments for this port range.
- ✓ **Apply Changes**: Click on “Apply Changes” to save the settings.
- ✓ **Reset**: Click on “Reset” to undo your changes.
- ✓ **Current Filter Table**: A table showing current port filtering.
- ✓ **Delete Selected**: Select and delete any listed port range.
- ✓ **Delete All**: Delete all the port ranges in the **Current Filter Table.**
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.5.2 IP Filtering

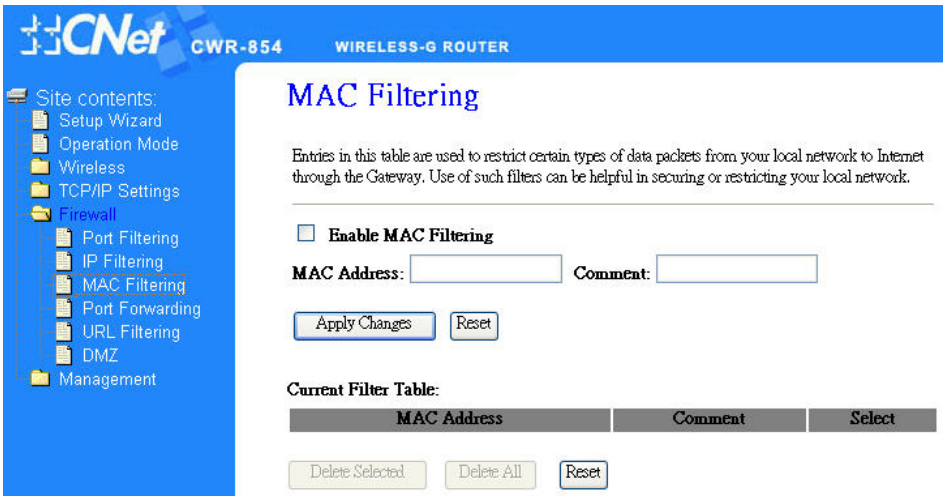
When enabled, LAN clients are blocked / filtered from accessing the Internet based on their IP addresses.

- ✓ **Enable IP Filtering**: Enable the IP Filtering function.
- ✓ **Local IP Address**: IP address that is to be blocked from accessing the Internet.
- ✓ **Protocol**: Select the protocol to be blocked UDP, TCP or both .
- ✓ **Comment**: This field is used for adding comments for each access control entry.
- ✓ **Apply Changes**: Click on “Apply Changes” to save the settings.
- ✓ **Reset**: Click on “Reset” to undo your changes.
- ✓ **Current Filter Table**: A table shows the list of current IP Addresses filtered.
- ✓ **Delete Selected**: Select and delete any IP Address in the **Current Filter Table**.
- ✓ **Delete All**: Delete all listed IP Address in the **Current Filter Table.**
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.5.3 MAC Filtering

When enabled, filtering will be based on the MAC address of LAN computers. Any computer with its MAC address on this list will be blocked from accessing the Internet.



- ✓ **Enable MAC Filtering**: Enable the MAC Filtering function.
- ✓ **MAC Address**: MAC Address that is to be blocked.
- ✓ **Comment**: Comments for this MAC Address.
- ✓ **Apply Changes**: Click on “Apply Changes” to save the setting.
- ✓ **Reset**: Click on “Reset” to undo your changes.
- ✓ **Current Filter Table**: A table showing current MAC Address filtering.
- ✓ **Delete Selected**: Select and delete any MAC Address in the **Current Filter Table**.
- ✓ **Delete All**: Delete all MAC Address in the **Current Filter Table.**
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.5.4 Port Forwarding

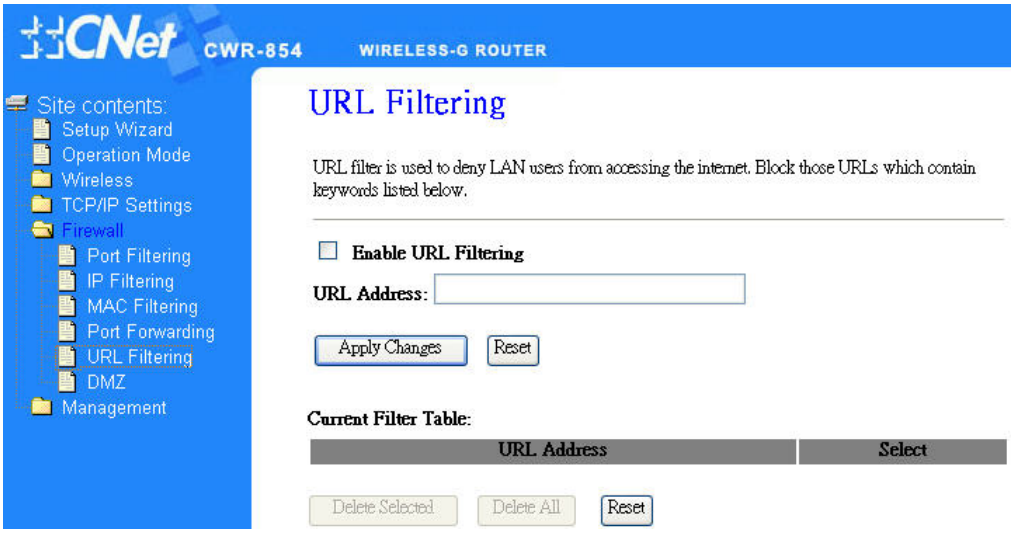
The Port Forwarding feature allows users to create Virtual Servers by re-directing a particular range of service port numbers (from the WAN port) to a particular LAN IP address.

- ✓ **Enable Port Forwarding**: Enable port forwarding function.
- ✓ **IP Address**: This is the private IP of the server behind the NAT firewall.
  (Note: You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.)
- ✓ **Protocol**: This is the protocol type to be forwarded. You can choose to forward "TCP" packet, "UDP" packet or "Both" (TCP + UDP).
- ✓ **Port Range**: The range of ports to be forward to the private IP.
- ✓ **Comment**: Add any comments for the rule.
- ✓ **Apply Changes**: Click on "Apply Changes" to save the settings.
- ✓ **Reset**: Click on "Reset" to undo your changes.
- ✓ **Current Port Forwarding Table**: A table showing the current Port Forwarding settings.
- ✓ **Delete Selected**: Select and delete any of the listed rules in the **Current Port Forwarding Table**.
- ✓ **Delete All**: Delete all Port Forwarding settings in the **Current Port Forwarding Table.**
- ✓ **Reset:** Click on "Reset" to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.5.5 URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.

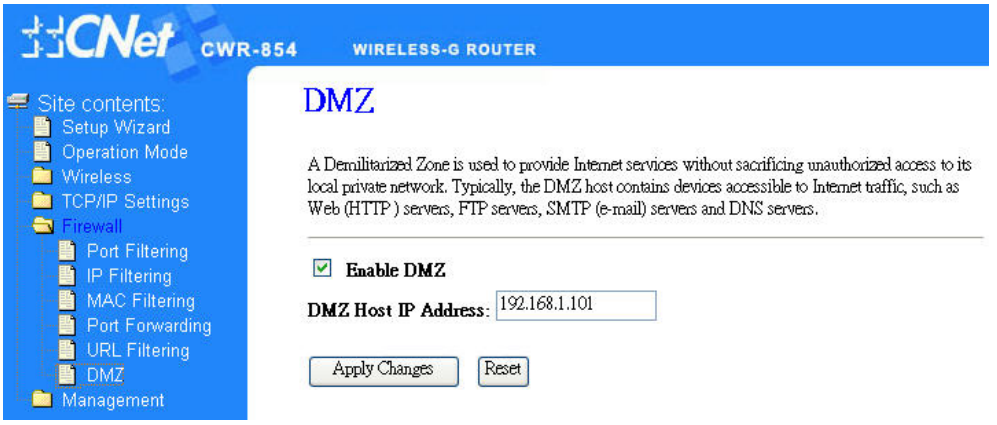


- ✓ **Enable URL Filtering**: Enable URL Filtering function.
- ✓ **URL Address**: Add one URL address.
- ✓ **Apply Changes**: Click on “Apply Changes” to save the settings.
- ✓ **Reset**: Click on “Reset” to undo your changes.
- ✓ **Delete Selected**: Select and delete any of the listed rules in the **Current Port Forwarding Table**.
- ✓ **Delete All**: Delete all Port Forwarding settings in the **Current Port Forwarding Table.**
- ✓ **Reset:** Click on “Reset” to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.5.6 DMZ

The DMZ feature allows one local user to be exposed to the Internet for special-purpose applications like Internet gaming or videoconferencing. When enabled, this feature opens all ports to a single station and hence renders that system exposed to intrusion from outside. The port forwarding feature is more secure because it only opens the ports required by that application..



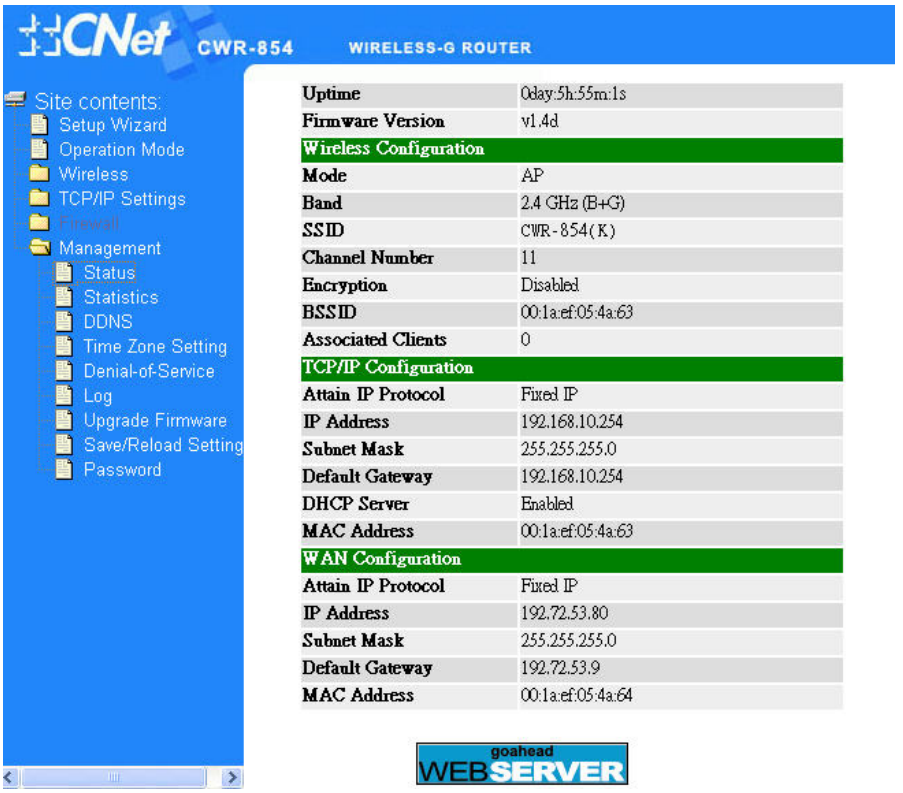
- ✓ **Enable DMZ**: Enable one PC to be exposed to the Internet.
- ✓ **DMZ Host IP Address**: Enter the computer's IP address in this field.
  (Note: You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.)
- ✓ **Apply Changes**: Click on "Apply Changes" to save the setting.
- ✓ **Reset:** Click on "Reset" to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6 Management

3.6.1 Status

The status page provides a brief read-only report for system, LAN and WAN configuration information. The data displayed may be changed depending on your current configuration.



System

- **Uptime**: The date/time shows how long the router has been powered on.
- **Firmware Version**: Show the current firmware version.

Wireless Configuration

- **Mode**: Shows the current operating modes.
- **Band**: Shows the current operating band.
- **SSID**: Shows the current SSID.
- **Channel Number**: Shows the current operating channel.
- **Encryption**: Shows the current encryption mode.
- **BBSID**: Shows the current BBSID on your Wireless LAN port.
- **Associated Clients**: Shows the number of associated clients .

TCP/IP Configuration

- **Attain IP Protocol**: Shows the IP protocol used on LAN
- **IP Address**: Shows the router's LAN interface IP address
- **Subnet Mask**: Shows subnet mask on your local network.
- **Default Gateway**: Shows the defined Default Gateway on your local network.
- **DHCP Server**: Shows the DHCP server status.
- **MAC Address**: Shows the MAC address on your LAN port.

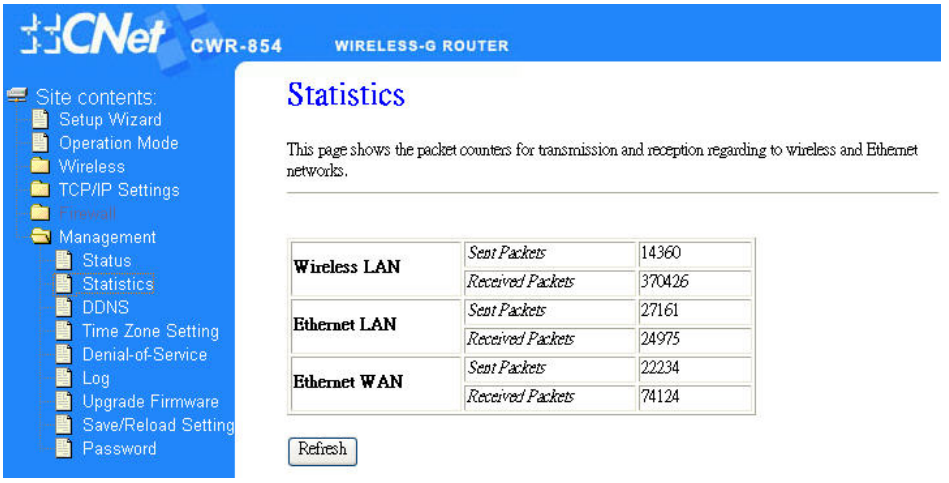
WAN Configuration

- **Attain IP Protocol**: Shows the IP protocol used on WAN.
- **IP Address**: Shows the router's WAN port IP address
- **Subnet Mask**: Shows subnet mask on your public network.
- **Default Gateway**: Shows the defined Default Gateway on your public network.
- **MAC Address**: Shows the MAC address on your WAN port.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.2 Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.



Wireless LAN

- **Sent Packet**: It shows the statistic count of sent packets on the wireless LAN interface.
- **Received Packet**: It shows the statistic count of received packets on the wireless LAN interface.

Ethernet LAN

- **Sent Packet**: It shows the statistic count of sent packets on the wireless LAN interface.
- **Received Packet**: It shows the statistic count of received packets on the wireless LAN interface.

Ethernet WAN

- **Sent Packet**: It shows the statistic count of sent packets on the wireless LAN interface.
- **Received Packet**: It shows the statistic count of received packets on the wireless LAN interface.

Refresh

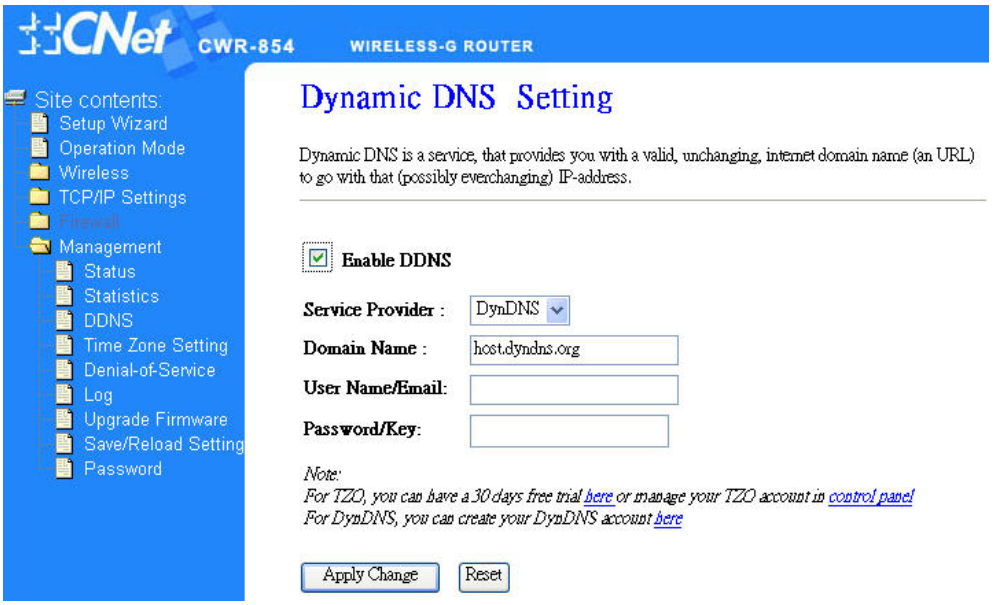
- Click the refresh the statistic counters on the screen.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.3 DDNS

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

(Note: make sure that you have registered with a DDNS service provider before enabling this feature.)

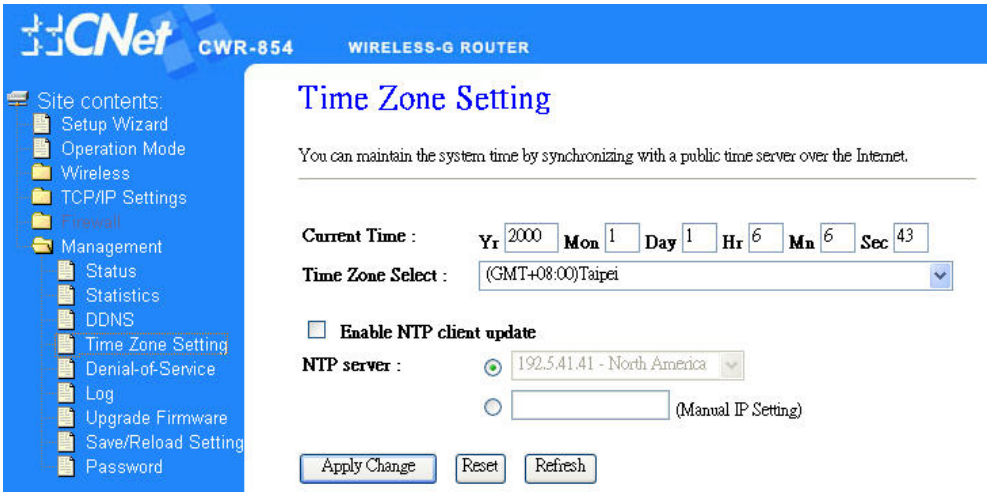


- ✓ **Enable DDNS**: Enable DDNS function.
- ✓ **Service Provider**: Select the DDNS Service Provider.
- ✓ **Domain Name**: Enter the Service Provider's Domain Name if needed.
- ✓ **Username/Email:** Enter the user name or Email address required to log into the DDNS account.
- ✓ **Password/Key**: Enter the password or Key number required to log into the DDNS account.
- ✓ **Apply Changes**: Click on "Apply Changes" to save settings.
- ✓ **Reset:** Click on "Reset" to undo your changes.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.4 Time Zone Settings

This wireless router provides a NTP (Network Time Protocol) client that can synchronize time with a configured NTP server. Pressing the Refresh Time button refreshes system timestamp and the Save/Time Sync buttons forces NTP client sync time with NTP server.

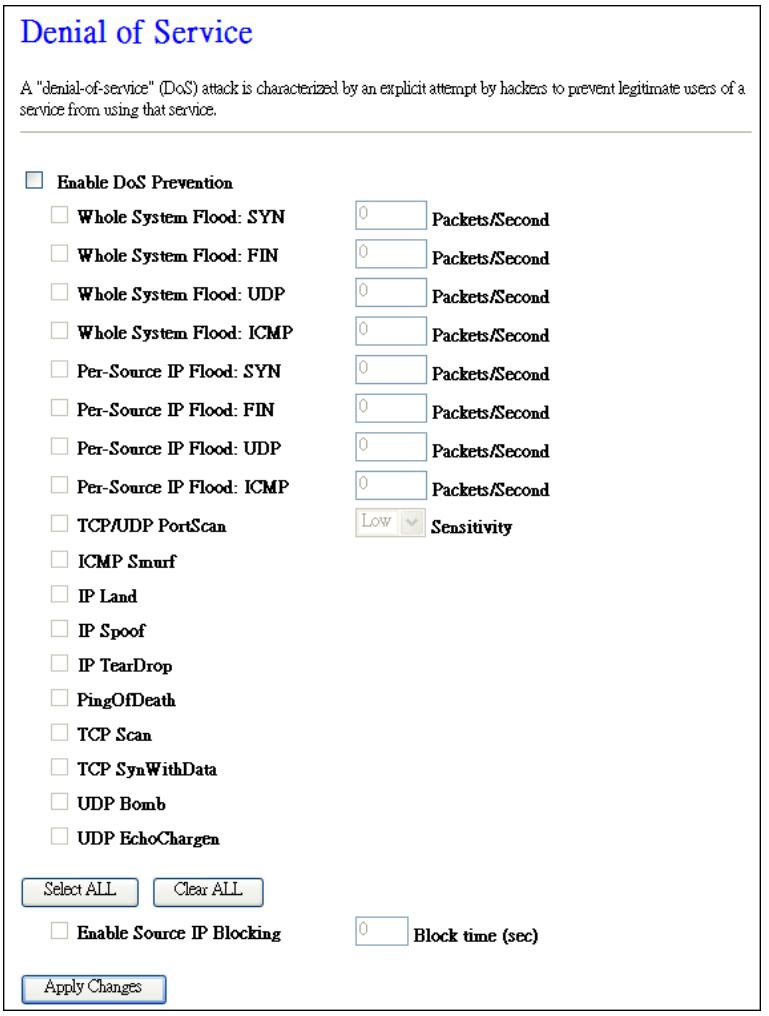


- ✓ **Current Time**: Show the current time and date of the router.
- ✓ **Time Zone Select**: Select the time zone of the country where this router is located.
- ✓ **Enable NTP client update**: Enable time zone update function.
- ✓ **NTP serve**r: Select the existing NTP servers by clicking the down arrow or manually assign time server address.
- ✓ **Apply Changes**: Click on “Apply Changes” to save settings.
- ✓ **Reset:** Click on “Reset” to undo your changes.
- ✓ **Refresh**: Get the date/time from NTP server again.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.5 Denial of Service (DoS Prevention)

This page is used to enable and setup protection to prevent attack by hacker's program. It provides more security for users.

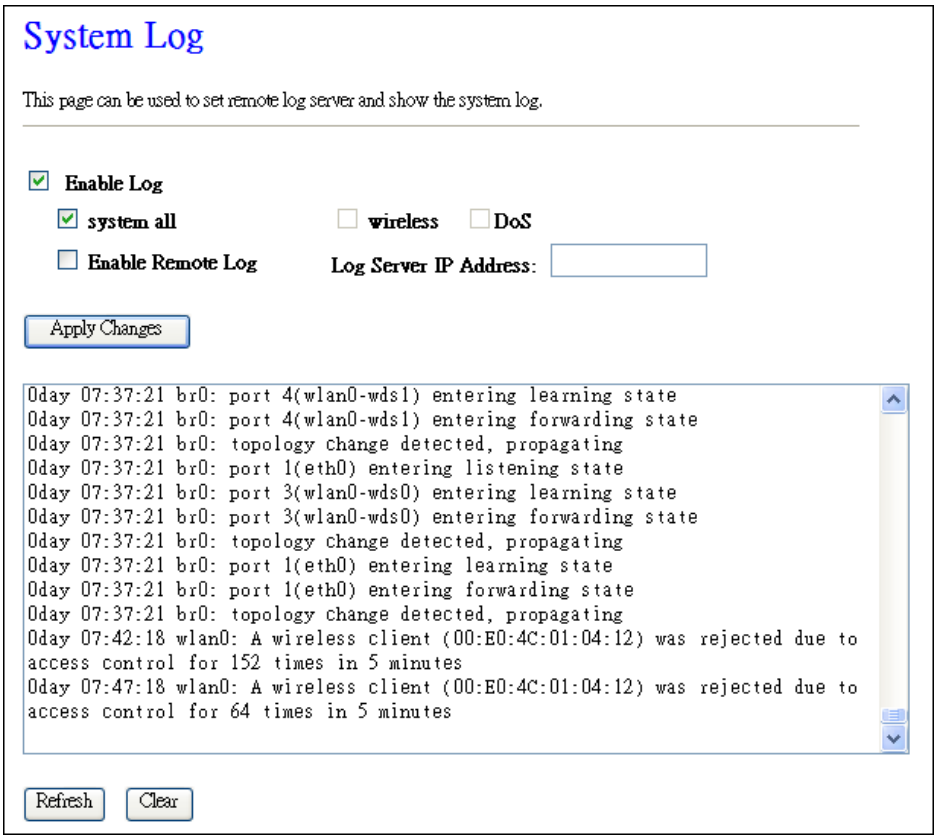


- ✓ **Enable DoS Prevention**: Click the checkbox to enable DoS prevention.
- ✓ **Whole System Flood / Per-Source IP Flood…**: Enable and setup prevention in details.
- ✓ **Select ALL**: Click the checkbox to enable all prevention items.
- ✓ **Clear ALL**: Click the checkbox to disable all prevention items.
- ✓ **Apply Changes**: Click on "Apply Changes" to save settings.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.6 Event Log

This wireless router supports System Log information. This data is useful for monitoring and troubleshooting the network.


System Log
This page can be used to set remote log server and show the system log.
Enable Log
system all
wireless
DoS
Enable Remote Log
Log Server IP Address:
Apply Changes
0day 07:37:21 br0: port 4(wlan0-wds1) entering learning state
0day 07:37:21 br0: port 4(wlan0-wds1) entering forwarding state
0day 07:37:21 br0: topology change detected, propagating
0day 07:37:21 br0: port 1(eth0) entering listening state
0day 07:37:21 br0: port 3(wlan0-wds0) entering learning state
0day 07:37:21 br0: port 3(wlan0-wds0) entering forwarding state
0day 07:37:21 br0: topology change detected, propagating
0day 07:37:21 br0: port 1(eth0) entering learning state
0day 07:37:21 br0: port 1(eth0) entering forwarding state
0day 07:37:21 br0: topology change detected, propagating
0day 07:42:18 wlan0: A wireless client (00:E0:4C:01:04:12) was rejected due to access control for 152 times in 5 minutes
0day 07:47:18 wlan0: A wireless client (00:E0:4C:01:04:12) was rejected due to access control for 64 times in 5 minutes
Refresh
Clear

- ✓ **Enable Log**: Enable the Log function.
- ✓ **System All**: Show all log of wireless broadband router.
- ✓ **Wireless**: Only show wireless log.
- ✓ **DoS**: Only show denied of Service log
- ✓ **Enable Remote Log**: Enable the Remote Log function.
- ✓ **Log Server IP Address**: Enter the Remote Log Server IP address when you use the Remote Log function. Logs can be sent to a remote server running a syslog daemon.
- ✓ **Apply Changes**: Click on “Apply Changes” to save settings.
- ✓ **Refresh**: Get the log data again.
- ✓ **Clear:** Click on “Clear” to clear all log data in the message box.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.7 Upgrade Firmware

The firmware on this wireless router can be easily upgraded.

Firmware Upgrade: Click on the **Browse** button to select the firmware and then click on the **Upload** button. After the firmware upgrade is completed, the router will restart automatically.

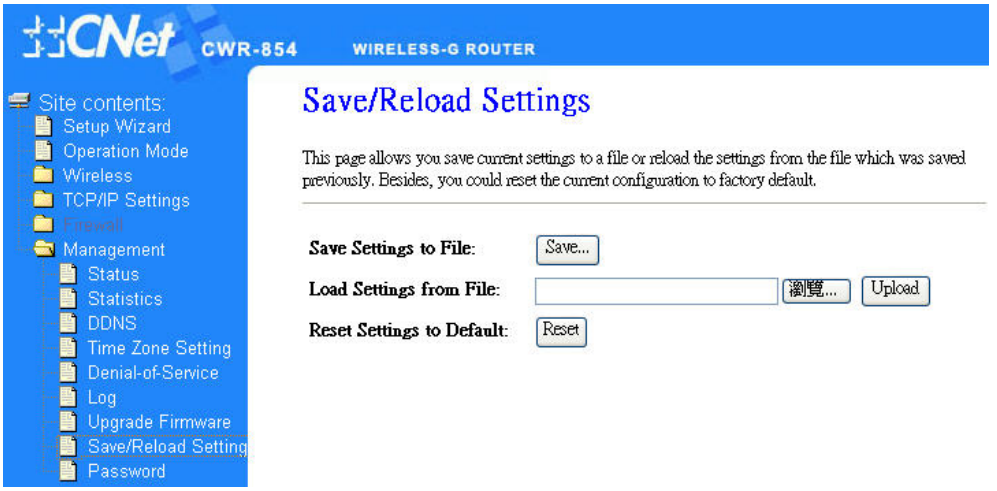
(Note: Do not power off the device while the firmware is being upgraded.)

- ✓ **Select File**: Enter the location and name of the file containing the new firmware. You can use the Browse button next to this field to browse for the file.
- ✓ **Upload**: Click to upgrade the router's firmware.
- ✓ **Reset:** Click on "Reset" to clear the Select File field.

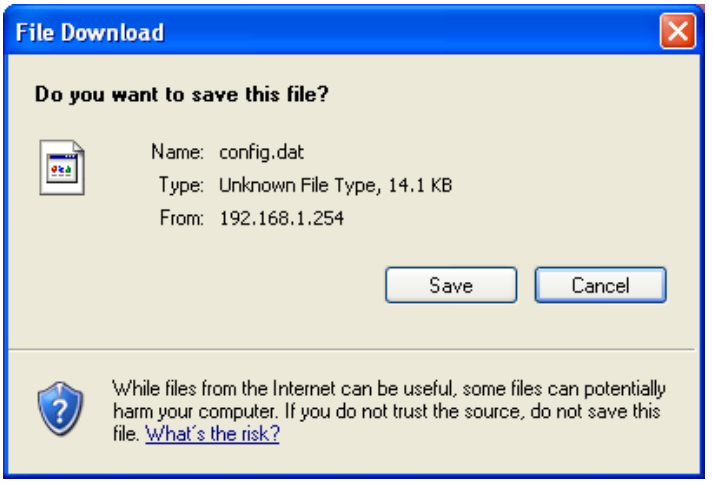
Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.8 Save / Reload Settings

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is specially useful in the event you need to reset the router to its default settings.



- ✓ **Save Settings to File**: Click on "**Save"** button to save the settings to a file "config.dat".


File Download
Do you want to save this file?
Name: config.dat
Type: Unknown File Type, 14.1 KB
From: 192.168.1.254
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

- ✓ **Load Settings from File**: Enter the location and name "config.dat" of the file which was saved. You can use the "**Browse"** button to browse to the location of the file.
- ✓ **Upload**: Click on "**upload"** button to upload previous settings**.**
- ✓ **Reset Settings to Default**: You can click on the "**Reset**" button to reset the current configuration to the factory default

Notes: The router will reboot automatically after firmware upgrade.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

3.6.9 Password

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

- ✓ **User Name**: Enter the new login user name. The user name can contain 1 to 30 characters and/or digits, and are case sensitive. **(Note: if you empty the user name, the password login protection will be disabled.)**
- ✓ **New Password**: Enter the new login password. The passwords can contain 1 to 30 characters and/or digits, and are case sensitive.
- ✓ **Confirmed Password**: Enter the new login password again.
- ✓ **Apply Changes**: Click on “Apply Changes” to save settings.
- ✓ **Reset:** Click on “Reset” to clear all fields.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

Appendix A: Troubleshooting

Symptom	Possible Causes	Things to Do
Inability to access the router	• Incorrect or incompatible wireless network configuration. For example, shared key authentication is configured on the wireless AP/Router and the wireless client is attempting open system authentication • Inadvertent media access control (MAC) address filtering • The wireless network name is not visible	• Verify that the wireless network configurations between the wireless client and wireless AP/Router are compatible. Make sure that the client system's network card is set to receive IP automatically. •Use "Ipconfig" utility to verify that the client is getting an IP address from the router: 1. Click Start > Programs and select Command Prompt. 2. Type ipconfig /all at the command prompt. 3. With default settings on the router, client should get an IP address in the range of 192.168.1.XX with a default gateway IP of 192.168.1.254.
	• The wireless AP/Router and wireless network adapter are not using the same 802.11 standard (for example, you are using an 802.11a network adapter and a 802.11g wireless AP/Router)	• Use the same 802.11 standard for wireless AP/Router and wireless network adapter.
	• Radio frequency (RF) interference from nearby devices such as cordless phones and Bluetooth devices	• Remove the device causing the interference.
	• Wireless client is at the periphery of the RF range of the wireless AP/Router	• Move the wireless client closer or re-locate the wireless AP/Router..
	• Improperly functioning or outdated wireless network adapter driver	• Obtain and install the most recent version of the wireless network adapter driver.
	• Cable failure (when wired to the router)	• Check the "Link" LED next to the port on the router. Make sure that Ethernet cables are connected properly.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

	• AP/Router is not power on	• Check the “Power” LED. Make sure that you’ve plugged in the power cord.
Intermittent connectivity	• IEEE 802.1X authentication is enabled on the wireless client and is not enabled on the wireless AP/Router • Improperly functioning or outdated wireless network adapter driver • Improperly functioning wireless AP/Router	• The symptom of this issue is when the wireless client loses connectivity every 3 minutes or so. Disable the authentication feature on the wireless client. • Obtain and install the most recent version of the wireless network adapter driver. Contact Technical Support
Incorrect, missing, or stale visible networks	• Improperly functioning or outdated wireless network adapter driver • Improperly functioning radio equipment on wireless AP/Router or wireless network adapter	• Obtain and install the most recent version of the wireless network adapter driver. • Run diagnostic functions on the wireless network adapter.
Wireless client has associated but there is no valid IP address configuration or no network connectivity	• Authentication problem • Incorrect encryption key • Bad or missing certificates • Improperly functioning wireless AP	• Verify that the wireless network configurations between the wireless client and wireless AP/Router are compatible. • If you are using a static WEP key, verify that it has been correctly configured. • Verify whether other computers connected to the wireless AP have the same problem. If all wireless clients of the same wireless AP/Router have the same problem, check the wireless AP/Router settings. • IEEE 802.1X authentication might be failing. Check it again.
Wireless connection problems when performing a suspend and resume with a laptop computer	• The Wireless Zero Configuration or Wireless Configuration services are not running • Improperly functioning or outdated wireless network adapter driver • On a laptop computer, the	• Check to see if the Wireless Zero Configuration or Wireless Configuration services are running with the sc query wzcsvc command. • With the Services snap-in, ensure that the Wireless Zero Configuration or Wireless Configuration services are

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

	wireless radio button might be in the off position	configured to start automatically. • A wireless network adapter driver failing in early stages of service startup may result in the Wireless Zero Configuration or Wireless Configuration service not initializing over that interface.
Client can't connect to the AP/Router's configuration utility.	• Wrong IP address	• Make sure that your PC is using an IP address within the correct range. It should be 192.168.1.2 to 192.168.1.254 for the default value. • Make sure that the address of the subnet mask is 255.255.255.0. • Try to use "Ping" utility to ping the AP/Router's IP, the default IP should be at 192.168.1.253 or 192.168.1.254 for AP and Router respectively.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

Appendix B: Frequently Asked Questions

Q1: What is wireless networking?
Ans: The term wireless networking refers to the technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

Q2: What is a wireless network made up of?
Ans: There are two kinds of wireless networks:
a. An ad-hoc, or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. (This is called "bridging")

Figure A1: Ad-Hoc or Peer-to Peer Networking.
Each computer with a wireless interface can communicate directly with all of the others.

b. A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.
There are two types of access points:
I. Dedicated hardware access points (HAP) such as Lucent's WaveLAN, Apple's Airport Base Station or WebGear's AviatorPRO. (See Figure A2). Hardware access points offer comprehensive support of most wireless features, but check your requirements carefully.

ii. Software Access Points which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network. (See Figure A3) The Vicomsoft InterGate suites are software routers that can be used as a basic Software Access Point, and include features not commonly found in hardware solutions, such as Direct PPPoE support and extensive configuration flexibility, but may not offer the full range of wireless features defined in the 802.11 standard.
With appropriate networking software support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa. Vicomsoft's solutions support file sharing using TCP/IP.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

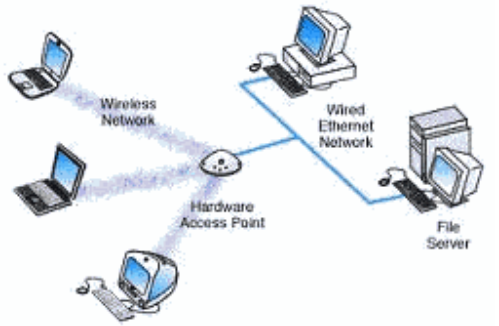


Figure A2: Hardware Access Point.
Wireless connected computers using a Hardware Access Point.

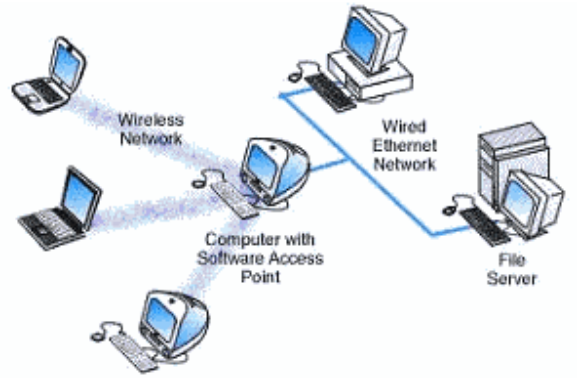


Figure A3: Software Access Point.
Wireless connected computers using a Software Access Point.

Q3: Can I mix wireless equipment from different vendors?
Ans: Because most wireless networking hardware vendors support the 802.11 standard they can inter operate. However, we recommend verification as the standard is a fairly recent one, and does specify two different methods for wireless communications; Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS or DS), which are not interoperable.
When purchasing wireless networking hardware from separate vendors be sure to obtain guarantees from the vendors that the hardware will interoperate and follows the standards.
Within a short time we expect all new wireless cards, like Ethernet cards, to become inexpensive, ubiquitous and totally interoperable.
Also of note is that the latest version of the standard defines 11mbps and 5.5mbps networking, with support for the older standard 1mbps and 2mbps speeds. This provides some compatibility with different or older equipment. Note that this new standard covers DS-type Networks, not FH types.
Software access points such as InterGate which uses the wireless interface of the host computer should have no compatibility issues with third party wireless hardware, as long as standards are followed. Typically wireless hardware is identified to the software as a network interface, and therefore can be used in the same way as any other network card.

Q4:If my computer is connected to a wireless LAN, can it communicate with computers on a wired LAN as well?
Ans: To do this you will need some sort of bridge between the wireless and wired network. This can be accomplished either with a hardware access point or a software access point. Hardware access points are available with various types of network interfaces, such as Ethernet or Token Ring, but typically require extra hardware to be purchased if your networking requirements change.
If networking requirements go beyond just interconnecting a wired network to a small wireless network, a software access point may be the best solution.
A software access point does not limit the type or number of network interfaces you use. It may

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

also allow considerable flexibility in providing access to different network types, such as different types of Ethernet, Wireless and Token Ring networks. Such connections are only limited by the number of slots or interfaces in the computer used for this task.
Further to this the software access point may include significant additional features such as shared Internet access, web caching or content filtering, providing significant benefits to users and administrators.

Q5: What is Roaming?
Ans: A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box.
Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

Figure A6: Roaming.
A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the best signal.

Not all access points are capable of being configured to support roaming. Also of note is that any access points for a single vendor should be used when implementing roaming, as there is no official standard for this feature.

Q6: What about security?
Ans: Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using special equipment.
To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels.
Also it should be noted that traditional Virtual Private Networking (VPN) techniques will work over wireless networks in the same way as traditional wired networks.
Section Two - Wireless Networking and the Internet

Q7: How can I use a wireless network to share an Internet connection?
Ans: Once you realize that wireless cards are analogous to Ethernet cards and that empty space

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

is analogous to Ethernet cabling, the answer to this question becomes clear. To share an Internet connection across a LAN you need two things:

(1) an Internet sharing hardware device or software program
(2) connection to a LAN

If your LAN is wireless, the same criteria apply. You need a hardware or software access point and a wireless LAN. Any computer equipped with a wireless network card running suitable Internet sharing software can be used as a software access point. (See Figure A8) A number of vendors offer hardware access points.

A hardware access point may provide Internet Sharing capabilities to Wired LAN computers, but does not usually provide much flexibility beyond very simple configurations. (See Figure A9)

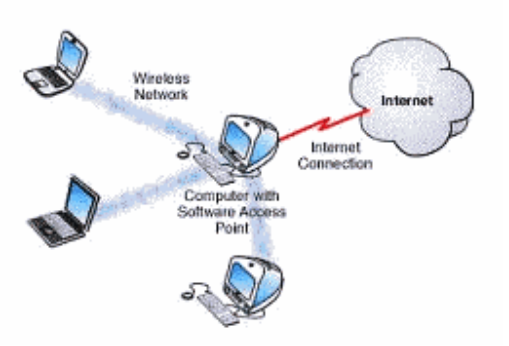


Figure A8: Software Access Point.
Wireless connected computers using a Software Access Point for shared Internet access.

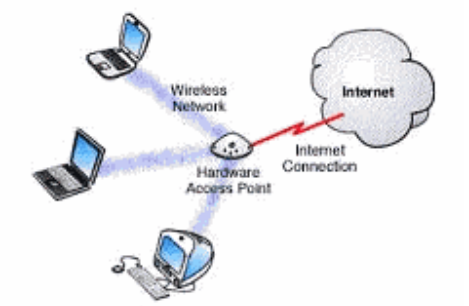


Figure A9: Hardware Access Point.
Wireless connected computers using a Hardware Access Point for shared Internet access.

Q8: How can I secure my wireless home network?

Ans: Here are 3 quick steps to help you secure your wireless network from unauthorized access. These steps are provided as general guidelines - for detailed help, please contact your hardware vendor.

1. Change the administrator password.
2. Change your SSID and turn off SSID Broadcasting
3. Enable WEP

Q9: What is Virtual Private Networking?

Ans: Typically, a Virtual Private Network (VPN) is defined as a group of two or more computer systems connected to a private network with limited public-network access that communicates securely over a public network, such as the internet: Security experts agree that VPNs include encryption, authentication of remote users or hosts, and mechanisms for hiding or masking information about private network topology from potential attackers on the public network:

Q10: What is encryption?

Ans: Encryption is a mathematical operation that transforms data from standard text to cipher text. Usually the mathematical operation requires that an alphanumeric key be supplied along with the standard text. The key plus standard text is processed by the encryption operation, which

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

produces secure scrambled text. Decryption is the opposite of encryption; it is the mathematical operation that transforms cipher text to standard text.

Q11: Why do I need a router?
Ans: The increased reliance on computers to store valuable information and the development of applications that share information over the internet through networked personal computers, in combination with the advent of computer hacking, has made information and network security an important issue. Typical analog modems and/or the higher-speed cable/DSL modems do not provide the necessary security to prevent someone from hacking into a computer. Having a device that provides network address translation (NAT) capability provides a simple solution to the hacking issue.

Q12: What is NAT?
Ans: Network Address Translation is used in a router to prevent hacking into the local area network (LAN). NAT substitutes a "private" IP address of devices located on the LAN side of the router with a new "public" IP address that is visible on the internet side of the router. By virtue of this simple implementation, any of up to 253 devices located on the LAN will be hidden from internet hackers. Only the router's IP address is visible on the internet.

Q13: Isn't NAT the same as "firewall"?
Ans: No. Though the term "firewall" has been used when describing a router's ability to hide the LAN IP addresses, a true firewall employs a technology called Stateful Packet Inspection (SPI). Firewalls provide a greater level of security and are generally more expensive than a NAT router. Firewalls give the administrator the ability to set up specific IP addresses or domain names that are allowed to be accessed, while refusing any other attempt to access the LAN. This is often referred to as filtering. Firewalls can also allow remote access to the private network through the use of secure login procedures and authentication certificates (VPN). Firewalls are used to prevent Denial of Service (DoS) attacks and can use software to provide content filtering to deny access to unwanted web sites.

Q14: Can the Access Point act as my DHCP Server?
Ans: No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

Q15: Can I run an application from a remote computer over the wireless network?
Ans: This will depend on whether or not the application is designed to be used over a network. See the application's user guide to determine if it supports operation over a network.

Q16: What is Ad-hoc?
Ans: An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

Q17: What is Infrastructure?
Ans: An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

Q18: What is WEP?
Ans: WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard.

Q19: How do I reset the Access Point or Router?
Ans: Press the Reset button on the back of the Access Point for about ten seconds. This will reset the unit to its default settings.

Q20: Does the Access Point function as a firewall?
Ans: No. The Access Point is only a bridge from wired Ethernet to wireless clients.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional

Q21: What is the maximum number of users the Access Point facilitates?
Ans: It depends on the volume of data and may be less if many users create a large amount of network traffic.

Q22: What is the maximum number of IP addresses that the Router will support?
Ans: The Router will support up to 253 IP addresses.

Q23: Where is the Router installed on the network?
Ans: In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.

Q24: Does the Internet connection of the Router support 100Mbps Ethernet?
Ans: The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

Q25: Does the Router support any operating system other than Windows 98, Windows Millennium, Windows 2000, or Windows XP?
Ans: Yes, at this time, provide technical support to setup, configuration or troubleshooting of any non-Windows operating systems.

Q26: When all else fails in the installation, what can I do?
Ans: Reset the Router by holding down the reset button until the Power LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available.

Q27: I am not able to get the web configuration screen for the Router. What can I do?
Ans :You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to direct connection to the Internet.

Q28: Can the Router act as my DHCP server?
Ans: Yes. The Router has DHCP server software built-in.

Q29: How to use Virtual Server in Wireless/Broadband Router?
Ans: It's also called Port forwarding. Virtual Server feature allows Internet users to access standard Servers on your LAN, via the Internet IP Sharer. Normally, Internet users would not be able to access a server on your LAN because your Server does not have a valid external IP Address.

Q30: Why Wireless/Broadband Router always has problem under Cable connection but not ADSL connection?
Ans: For ADSL, one subscriber shares one line. If your ISP provides you a 512K account then you can enjoy the full 512Kbps on your side. But Cable is different. Many subscribers share the same line. For example, the bandwidth of Cable is 1.5Mbps. If there are 25 users accessing the Internet at the same time then the bandwidth of each user is 1500K/25 near 60K. The speed is just like the traditional modem connection. If there are only 5 users on line at this moment then each user can share the bandwidth to nearly 300K (1500K/5). So, the speed over ADSL is more stable than Cable. The access will hang up when the traffic is heavy over the Cable. It is the reason why many problems only happen over Cable.

Created with nitroPDF professional
download the free trial online at nitropdf.com/professional